

LA PROTECCIÓN DE LOS DATOS DEL MENOR EN EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

RAQUEL PÉREZ DÍAZ

Doctora. Profesora Asociada de Derecho Civil de la Universidad de Oviedo. Abogada

RESUMEN

A consecuencia del uso de la informática, he constatado la necesidad de abordar el estudio del derecho de la personalidad como es el la protección de datos del menor en España, en la Unión Europea, toda vez que la utilización de estas nuevas tecnologías conlleva que se traten y cedan sus datos desde muy temprana edad, generando problemas debido principalmente a la falta de plena capacidad y ser un colectivo que se encuentra en formación, por lo que precisa una especial protección.

Palabras clave: menor; protección de datos personales; imagen; nuevas tecnologías; internet; dispositivos móviles; redes sociales.

THE DATA PROTECTION OF THE MINOR IN THE USE OF THE TECHNOLOGIES OF INFORMATION AND COMMUNICATION (TECHNOLOGY ICT)

ABSTRACT

And consequence of the use of computers, I have seen the need to address the study of a new right of personality is the data protection of the child in Spain, the European Union, every time that the use of these new technologies brings with it that they are processed and transferred your data from an early age, generating problems due mainly to the lack of full capacity and be a collective that is in training, so it requires special protection.

Key words: minor; protection of personal data; self-image; new technologies; internet; mobile devices; social networks.

SUMARIO

1. LA PROTECCIÓN DE DATOS PERSONALES DEL MENOR. 2. REGULACIÓN EN ESPAÑA. 2.1.1. La protección de datos de carácter personal como derecho fundamental 2.1.2. Ámbito de aplicación de la protección de los datos personales. 2.1.3 Concepto de dato personal. La imagen del menor. 2.1.4. Conceptos de fichero, tratamiento y cesión de datos. Ámbitos de tratamiento y cesión de datos personales del menor. 2.1.5. El deber de informar la recogida y el tratamiento de los datos personales del menor. 2.1.6. El consentimiento del menor en el tratamiento de sus datos personales. 2.2. REGULACIÓN EN LA UNIÓN EUROPEA. 2.2.1. El marco normativo vigente en materia de protección de datos personales. 2.2.2. El Reglamento general de protección de datos de la UE 2016/679, de 27 de abril de 2016. 2.2.3. El consentimiento del menor en el tratamiento de sus datos personales. 2.2.4. Otras medidas dirigidas a la protección del menor. El derecho al olvido. 3. BIBLIOGRAFÍA

1. LA PROTECCIÓN DE LOS DATOS PERSONALES DEL MENOR

1.1. REGULACIÓN EN ESPAÑA

En relación al derecho a la protección de datos de carácter personal o habeas data, en España, se lleva a cabo su regulación específica con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RLOPD). Ahora bien, como consecuencia del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), en fecha 24 de noviembre de 2017 se ha aprobado en el Congreso de los Diputados el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal con el fin de adaptarse al mismo (PLOPD) que entrará en vigor como nueva LOPD el 25 de mayo de 2018.

1.1.2. La protección de datos de carácter personal como derecho fundamental

El artículo 18.4 de la Constitución Española (CE) obliga a *“limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*, pero no fue hasta el año 1992 cuando existió normativa específica en este ámbito, primero la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal –LORTAD– y posteriormente la LOPD que ha transpuesto la Directiva 95/46/CE y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos; aunque, quien verdaderamente ha procedido a cumplimentar y desarrollar los aspectos más importantes de la citada ley es el RLOPD.

El desarrollo legislativo de este derecho fundamental está en la LOPD, siendo su objeto (art. 1) *“Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*.

Para calificar la protección de datos como un derecho fundamental de la personalidad, diferenciado definitivamente del derecho a la intimidad, hay que acudir a la Sentencia del Tribunal Constitucional (STC) 292/2000, de 30 de noviembre¹, a partir de la cual se consagra como *“Un derecho fundamental independiente y autónomo con respecto al derecho a la intimidad”* exige una regulación completa y adecuada y su contenido consiste en *“Un poder de disposición y de control sobre los datos personales, que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o usos. Estos poderes de posición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento informático o no de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos”*.

¹ Realiza una análisis en profundidad sobre las diferencias entre el derecho a la intimidad y a la protección de datos.

Pero, la LOPD ha sido objeto de reiterada crítica doctrinal², y en mi opinión con razón, pues no dedica ningún precepto a regular específicamente la protección de datos personales de los menores de edad, los cuales, se han regido por las reglas generales de la citada ley, tan sólo contiene dos referencias puntuales: una, en su art. 7. 6 en el contexto de los denominados “*datos especialmente protegidos*”³ y otra, en el art. 22. 4 al tratar los ficheros policiales, de forma incluso aún más tangencial⁴. Donde sí se encuentra por primera vez una norma que regula la protección de datos personales de los menores de edad es en el RLOPD concretamente en su art. 13 donde se recoge las condiciones para prestar el consentimiento por parte de los menores en el tratamiento de sus datos personales. En ese sentido, también el PLOPD hace referencia al menor en su art. 7 regulándose expresamente al consentimiento de los menores de edad.

2.1.2. Ámbito de aplicación de la protección de los datos personales

En España, el ámbito de aplicación de la protección de datos de carácter personal se establece en los art. 2.2.a) LOPD, art. 4.a) RLOPD y en el art. 2.2.a) PLOPD⁵ en todos ellos se excluyen “*los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas*” indica el Reglamento además que “*sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares*”. Asimismo, el art. 2.2 del RLOPD desarrolla que “*No será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales*”.

Por ende, nuestra normativa no protege los datos de personas jurídicas; tampoco los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en redes profesionales -cuando constan únicamente nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales-; ni los ficheros con datos relativos a empresarios individuales cuando se haga referencia a ellos en su calidad de comerciantes, industriales o navieros; de tal manera que la información de relaciones profesionales no forma parte nuclear de la privacidad de las personas. En consecuencia, lo que respecta al tratamiento de datos relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto, nadie puede invocar la protección del presente Reglamento. Ello, también es de aplicación

² GÓMEZ-JUÁREZ SIDERA reclamaba que “...en el propio texto de la LOPD se haga una mención específica a los datos de los menores de edad en el apartado relativo a la obtención del consentimiento para el tratamiento de los datos que incorpore las interpretaciones de la AEPD al respecto”. GÓMEZ-JUÁREZ SIDERA, I, “Reflexiones sobre el derecho a la protección de datos de menores de edad y la necesidad de su regulación específica en la legislación española”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 11, 2006, p. 86.

³ La primera referencia a los menores de edad en la LOPD se realiza en el art. 7. El apartado 6 de dicho art., se refiere a los sujetos que no tienen capacidad jurídica suficiente para prestar su consentimiento, entre los que están menores, y los incapacitados. El consentimiento se requiere expreso cuando se autoriza el tratamiento de dichos datos especialmente protegidos, pero el art. 7.6 LOPD establece que no será necesario el consentimiento expreso cuando el mismo “*sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento*”.

⁴ Art. 7.6 “*Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento*” y que, a tales efectos, “*se considerará especialmente la edad del afectado y el carácter de los datos almacenados*”.

⁵ Art. 2.2.a “*Esta ley orgánica no será de aplicación: a) A los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*”.

cuando el nombre de la persona jurídica incluya los nombres de una o más personas físicas. Ahora bien, el problema surge con las redes generalistas, pues tienen un mayor nivel de riesgo al ofrecer tanto información profesional como vivencias o aficiones como por ejemplo Muspace, que si bien es una red generalista, dispone de un grupo formado por artistas que la aprovechan para dar a conocer sus trabajos ante el público en general. A sensu contrario, sí estarán incluidos en la normativa, los datos de carácter personal o doméstico utilizados por los usuarios en el servicio de red social como una plataforma de colaboración con una empresa para una finalidad comercial⁶ o como un medio para desarrollar una finalidad de carácter político o social, que no son finalidades personales o domésticas.

Por su parte, el Reglamento General de Protección de Datos (RGPD), también excluye de su ámbito de aplicación material los tratamientos de datos personales que lleve a cabo una persona física en el ejercicio de sus actividades exclusivamente personales o domésticas, y precisa con acierto “*siempre que no tengan un interés lucrativo*” art. 2.2.d)⁷. Hay que recordar, que en las redes sociales, esta cuestión no es baladí, pues la mayoría de los tratamientos que llevan a cabo los usuarios afecta a la esfera familiar y de amistad, y por tanto, están excluidos de la aplicación de dicha normativa. Sin embargo, tal y como viene interpretándose jurisprudencialmente y doctrinalmente hay una excepción, cual es la no aplicación la exención doméstica cuando los datos sean especialmente sensibles, por referirse al estado de la salud, la religión, la afiliación política, la raza o aspectos de la vida sexual de las personas, o el caso de la difusión del sexting ajeno en determinados ficheros informáticos que permiten su tratamiento organizado, tales como páginas web, portales colaborativos o perfiles públicos de redes sociales o Web 2.0, infringiendo el derecho a la protección de datos personales y pudiendo ser castigado conforme a la LOPD.

Conforme señala TRONCOSO REIGADA en los casos en que el servicio de redes sociales es utilizado por los usuarios afectando a una aceptación indiscriminada de peticiones de amistad, el perfil o los contactos se encuentran abiertos para todos los usuarios de la red social o la información puede ser indexada a través de motores de búsqueda fuera de la propia red; con lo cual, el usuario debe ser considerado como responsable del tratamiento, aplicándose el mismo régimen que en la publicación de datos personales en otras plataformas tecnológicas abiertas en Internet⁸ y la consecuencia es que se le puede exigir las obligaciones y derechos que le otorga la legislación de protección de datos. Un caso típico y habitual de tratamiento personal o doméstico es la realización de fotografías de grupo de menores en centros educativos por parte de los padres; ahora bien, si se publican en Internet en abierto constituyen una cesión indiscriminada de datos personales con lo que sí sería de aplicación la misma.

Por todo lo anterior, se puede concluir que los usuarios de redes sociales tienen la consideración de afectados o interesados al ser las personas titulares de los datos que son objeto de tratamiento (art. 3.e) de la LOPD). De cualquier modo, no se aplica la LOPD y

⁶ El Dictamen 5/2009 del Grupo de Trabajo (GT) del Artículo 29 precisa en qué circunstancias las actividades de un usuario de servicios de redes sociales no están cubiertas por la “*exención doméstica*”. Una preocupación de este grupo de trabajo es la difusión y utilización de la información disponible en los servicios de redes sociales con fines secundarios. Muchas redes sociales especializadas son básicamente redes de profesionales, como Linkedinn, que quiere favorecer las relaciones entre profesionales, o Ryze.com. que hace conexiones de empresas para resolver sus necesidades.

⁷ El Considerando 15 del Reglamento pone como ejemplo de tratamientos personales o domésticos la correspondencia o llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por ello, sin conexión alguna con una actividad profesional o comercial. Sin embargo, precisa que esta exención no debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.

⁸ TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, p. 1697.

el RLOPD a los datos que quedan incluidos en la esfera familiar o domésticas salvo los sensibles y aquellos referidos a personas fallecidas, ello sin perjuicio de que las personas vinculadas a aquellas puedan dirigirse a los responsables de los ficheros que contengan datos de aquellas personas con la finalidad de notificar el óbito, aportando acreditación suficiente de la persona fallecida y solicitar, en su caso, la cancelación de los datos (art. 2.4)⁹. Tampoco la Directiva 95/46/CE, de 24 de octubre (art. 2.a) ni el RGPD resuelven esta cuestión¹⁰. Sin embargo, el PLPD aunque también excluye el tratamiento de datos de las personas fallecidas, su art. 3 permite que los herederos puedan ejercitar el acceso a los mismos, así como su rectificación o supresión y ello conforme a las instrucciones del fallecido¹¹. La Sentencia del TJUE de 11 de diciembre de 2014 hace una interpretación amplia del concepto de “ejercicio de actividades exclusivamente personales o domésticas”¹².

2.1.3. Concepto de dato personal. La imagen del menor

Siguiendo las directrices de la Directiva 95/46/CE, de 24 de octubre, los arts. 3 LOPD y 5 del RLOPD establecen una serie de definiciones relativas a los sujetos, objetos, operaciones y demás aspectos relacionados con la materia que deben concurrir para posibilitar la aplicación de dicha regulación protectora, las cuales igualmente son recogidas en el precepto 4 del RGPD.

⁹ En la misma dirección la LO 1/1982, de 5 de mayo, prevé las personas que pueden ejercer las acciones de protección del derecho a la intimidad de la persona fallecida y solicitar la cancelación de su perfil personal la persona designada en testamento a tal efecto, los familiares directos o el MF (arts. 4 y 5). Ha existido una evolución en la posición de las redes sociales sobre el mantenimiento de la publicación del perfil personal de una persona tras su muerte. Algunas redes sociales, desde un planteamiento patrimonialista de la propiedad intelectual de lo publicado en su plataforma, continuaban con la publicación del perfil personal de los fallecidos, lo mismo que ocurría con los blogs escritos por personas fallecidas, por ejemplo con el perfil del periodista William Bemister, a pesar de las reclamaciones de su hermana. En nuestro país también se planteó con la continuidad de la publicación de los datos y conversaciones privadas de Marta Del Castillo el derecho a la intimidad. TRONCOSO REIGADA, ob. cit., p. 67. “No es agradable que cada vez que tecleas el nombre de un ser querido en Google aparezca una multa de tráfico, la foto de su orla o comentarios desagradables en blogs o redes sociales. Nosotros hacemos que esos enlaces desaparezcan y ayudamos también a gestionar todas las cuentas y perfiles que hayan podido quedar abiertas”. Se calcula que unos 30 millones de perfiles de Facebook pertenecen a personas fallecidas en todo el mundo. Como borrar el pasado en Internet <http://sociedad.elpais.com/sociedad/2014/05/17/actualidad/1400358691-542355.html>. RAQUEL VIDALES.

¹⁰ Considerando 27. “El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas”.

¹¹ Art. 3. “Datos de las personas fallecidas. 1. Los herederos de una persona fallecida que acrediten tal condición mediante cualquier medio válido conforme a Derecho, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. 2. El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos. 3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo.”

¹² Dice que “la utilización de un sistema de cámara de vídeo, que da lugar a la obtención de imágenes de personas que luego se almacenan en un dispositivo de grabación continuada, como un disco duro, sistema de vídeo vigilancia instalado por una persona física en su vivienda familiar con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre también el espacio público, no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la citada disposición de la Directiva”.

De modo tal, que el concepto de dato personal se define con carácter general en el art. 3.a) de la LOPD y se refiere a “*Cualquier información concerniente a personas físicas identificadas o identificables*”, siendo completada y clarificada su definición en el art. 5.1.f) del RLOPD al añadir “*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*”. Hay que tener en cuenta que la información personal que contiene los datos personales se refiere tanto a personas identificadas como no identificadas, lo que nos lleva al art. 5.1.o) RLOPD para saber que se considera por persona identificable “*Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social*” y, por no identificable “*Aquella cuya identificación requiere plazos o actividades desproporcionados*”. Finalmente, también el RGPD en su art. 4.2) define dato personal como “*Toda información relativa a un interesado*” y aunque pudiera pensarse que es la definición más restrictiva hasta ahora, es todo lo contrario, pues incluye además como nuevos datos personales la IP, las cookies o los datos de pseudónimos. Asimismo, añade información genética para poder identificar a una persona¹³.

Con ello, y a sensu contrario, se puede concluir que todos aquellos datos que se encuentren disociados no se consideran personales y conforme al art. 5.1.e) RLOPD será “*Aquél que no permite la identificación de un afectado o interesado*”, y en este caso, no se aplicará la regulación de protección de datos dado que se trata de datos pertenecientes a una persona que no se puede identificar.

Por su parte, la APED¹⁴ va más allá, y define dato personal como “Una información que nos identifica o nos puede identificar como el nombre y los apellidos, la fecha de nacimiento, la dirección postal o de correo electrónico¹⁵, el número de teléfono¹⁶, el DNI¹⁷, la matrícula de los vehículos¹⁸, las IP incluyendo las del móvil¹⁹, los cookies, captación de imágenes mediante cámaras de video vigilancia²⁰, un dibujo realizado a una

¹³ “Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.”

¹⁴ AEPD @navega seguro, p. 2.

¹⁵ Considera SEMPERE, que la identificación de una persona mediante el correo electrónico es bastante discutible, dependerá si ese correo electrónico se ha usado el nombre y apellidos de una persona, pues en caso contrario, la cuestión se vuelve bastante dudosa, por ejemplo a efectos de identificación no es lo mismo un juanmartínez@gmail.com que un correo totalmente inventado trasteando@hotmail.com. SEMPERE SAMANIEGO J., *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, libro publicado mediante Licencia Creative Commons Reconocimiento- No Comercial- Compartir igual CC BY-NC- SA, <http://es.linkedin.com/pub/fco-javier-sempere-samaniego/19/4bb/bba>, p. 103.

¹⁶ Dictamen 285/2006, de la AEPD sobre la prestación de un servicio tele taxi.

¹⁷ Dictamen 334/2008, de la AEPD sobre la creación de un fichero cuyo único dato es el DNI o NIF.

¹⁸ Dictamen 425/2006, de la AEPD sobre la naturaleza de los datos contenidos en la placa de matrícula de un vehículo y el nivel de protección exigido por la Ley de dichos datos.

¹⁹ Dictamen 4/2007 sobre concepto de datos personales GTP D del Art. 29, p. 18-19. Si bien la IP lo que puede es identificar al titular de la línea pero no a quien esté utilizando el ordenador de esa IP, por lo que la argumentación de la AEPD tendría que ser matizada, considera SEMPERE, ob. cit., p. 106. En este sentido, apoya esta argumentación la STS 987/2012 de 3 de diciembre que procede a anular una condena a dos personas que habían cometido una estafa informática en base a que la identificación de los acusados mediante la IP no es prueba suficiente para acreditar la comisión del delito. Por el contrario la Audiencia Nacional también se ha manifestado sobre el carácter de dato personal la IP en el llamado “*Caso Promusicae*” basándose para ello en los mismos argumentos que la AEPD es decir que la IP es un dato de carácter personal y que Internet, al no tener la consideración de fuente accesible al público, determina que es necesario el consentimiento para tratar ese dato personal, que no se puede aplicar la excepción de informar del art. 5.5 RLOPD, p. 107.

²⁰ Dictamen 4/2007 sobre concepto de datos personales, GTPD del Art. 29, p. 8.

niña durante una prueba neuropsiquiátrica²¹, una fotografía o una grabación telefónica de nuestra voz²², el valor de una vivienda asociado a su propietario²³, el registro de llamadas de un teléfono²⁴, el sistema de localización de un taxi²⁵, y muchos otros datos que usamos a diario y que constituyen información valiosa que podría permitir identificar a una persona ya sea directa o indirectamente”. Toda esta información nos permite desarrollar nuestra actividad cotidiana, como puede ser inscribir a nuestros hijos en el colegio, recibir atención sanitaria, realizar llamadas telefónicas o disfrutar de nuestro ocio.

Por la jurisprudencia de la Unión Europea, resulta de particular interés la Sentencia de 6 de noviembre de 2003 (Lindqvist Asunto c-101/01)²⁶ del Tribunal de Justicia de la Unión Europea (TJUE) en la que se establecen con claridad los criterios a aplicar sobre la protección de datos en Internet; y sin duda, se incluye el nombre de una persona junto a su número de teléfono u otra información relativa a sus condiciones de trabajo o a sus aficiones como dato personal conforme al art. 2.a) y 3.1 de la Directiva 95/46.

Como en la normativa de protección de datos no se define la imagen como dato personal, nos surge la cuestión de si es o no un dato personal. Cuando los usuarios de las redes sociales vuelcan una imagen, ésta tiene la consideración de dato personal, pudiendo incluso afectar al derecho fundamental a la propia imagen cuando se trata la de un tercero. Aun así, naturalmente en la mayoría de los casos, esas imágenes se mantienen en el ámbito de los amigos o conocidos, por lo que son considerados ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas como se recoge en el art. 2.2 a) LOPD. En virtud de esta exención doméstica, en principio, cabe excluir a priori las imágenes del marco de aplicación de la LOPD ya que normalmente son empleadas con una finalidad privada o doméstica.

No obstante, para la APED la imagen es dato personal siempre y cuando permite la identificación de las personas que en ella aparecen. Y en este sentido, es relevante el Informe 0194/2009 elaborado como consecuencia de la consulta ante la publicación no consentida en la página web de un centro escolar de fotos de una alumna con motivo de la realización de diversas actividades extraescolares²⁷. Pero como bien apunta REBOLLO

²¹ Dictamen 4/2007...ob. cit., p. 9.

²² Dictamen 4/2007...ob. cit., p. 8.

²³ Dictamen 4/2007...ob. cit., p. 9.

²⁴ Dictamen 4/2007...ob. cit., p. 12.

²⁵ Dictamen 4/2007...ob. cit., p. 12.

²⁶ La Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). A finales de 1998, creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que pudiera resultarles útil. Dichas páginas contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre de pila, acompañado, en ocasiones, del nombre completo. Además, describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y que se encontraba en situación de baja parcial por enfermedad. La Sra. Lindqvist fue condenada a pagar una multa de 4000 SEK (aproximadamente 450 euros) por haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datatillsynsmyndigheten (organismo público para la protección de los datos transmitidos por vía informática), por haberlos transferido a países terceros sin autorización y por haber tratado datos personales delicados (una lesión en un pie y una baja parcial por enfermedad). Nota de prensa publicada en <http://curia.europa.eu/es/actu/communiques/cp03/aff/cp0396es.htm>.

²⁷ Las imágenes a las que se refiere la consulta tendrán la consideración de datos de carácter personal en caso de que las mismas permitan la identificación de las personas que en ellas aparecen, no encontrándose amparadas por la LOPD en caso contrario. Siendo la imagen un dato personal, en los términos vistos, la toma de fotos de los alumnos efectuada por el colegio constituye, por ende, un tratamiento de datos personales, tal y como prevé el art. 3 de la LOPD. En lo que se refiere al tratamiento de datos de carácter personal, entre las obligaciones del responsable del fichero, en el presente caso el centro escolar, está la de obtener el consentimiento del interesado para el tratamiento o cesión de los datos y la de informar sobre los derechos que les asisten, así como sobre la identidad y dirección del responsable y sobre el uso que se va a dar a esos datos.

DELGADO²⁸ no hay que olvidar que la imagen puede tener dos vertientes distintas y, por ende, ser incluida en dos derechos distintos. El derecho a la propia imagen o el derecho de protección de datos, la elección de uno u otro será en función de las circunstancias y derechos que en cada caso resulten afectados, pues la captación de una fotografía, dependiendo del lugar, lo fotografiado y la situación concreta de la persona puede o no resultar intromisión ilegítima en el derecho a la propia imagen o en el derecho a la protección de datos. Lo significativo es la existencia de los requisitos necesarios que posibiliten configurar cada supuesto concreto, bien el derecho a la propia imagen, o bien en su caso la imagen como dato. Por consiguiente, para que las imágenes que constan en videos o fotografías que permiten la identificación de las personas que en ellas aparecen sean datos personales amparados por la LOPD habrá que examinar si la toma y difusión de ellas realizadas por particulares está incluida o excluida de la aplicación de la normativa de protección de datos; quedará incluida cuando la difusión de la imagen no se reduce a un número cerrado de contactos sino que se difunde de manera indiscriminada, es decir, cuando los contactos personales se encuentran abiertos para todos los usuarios de la red social o cuando la información personal puede ser indexada a través de motores de búsqueda fuera de la propia red; y excluida, cuando se difunde entre contactos cerrados o entre particulares en los que existe una relación de amistad o familiar. En esa línea, se pronuncian la Sentencia de la Audiencia Nacional (SAN) de 15 de junio de 2006²⁹ o la SAN Sala de lo Contencioso Administrativo, Sección 1ª, de 20 de abril de 2009³⁰. En cualquier caso, la imagen no se considera dato sensible y conforme a los casos previstos en el art. 7 del RLOPD³¹, es fuente accesible al público pudiendo ser consultada por cualquier persona.

En definitiva, la imagen de una persona (mayor o menor de edad) al igual que otras manifestaciones de su identidad (la voz o el nombre) se consideran datos de carácter personal cuando no exista limitación alguna para acceder a la publicación de las fotos o vídeos en Internet y se regulará por la LOPD y el RLOPD. Aunque también puede ser abordada desde el punto de vista del derecho a la propia imagen reconocido como derecho fundamental en el art. 18.1 CE siempre y cuando el sujeto sea reconocible. En la práctica, y a pesar de la doble vertiente parece preferirse más la defensa de la imagen desde la regulación de la protección de datos de carácter personal debido a la mayor simplicidad y gratuidad del procedimiento sancionador que se inicia por la AEPD.

²⁸ REBOLLO DELGADO, L., *La imagen como dato*. Anuario Facultad de Derecho. Universidad de Alcalá de Henares. Servicio de Publicaciones, nº 2, 2009, <http://hdl.handle.net/10017/6442>, pp. 177-201.

²⁹ “(...) Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos”.

³⁰ “La imagen de una persona es un dato personal al que se aplica la LOPD cuando está recogida en ficheros de datos personales, por consiguiente la LOPD será de aplicación a las imágenes consentidas en páginas web, portales colaborativos de público acceso -como puede ser Youtube- o perfiles de redes sociales accesibles a un elevado número de usuarios”.

³¹ Art. 7 “Fuentes accesibles al público: 1. A efectos del artículo 3, párr. j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público: a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre. b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica. c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional. d) Los diarios y boletines oficiales. e) Los medios de comunicación social. 2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.”

2.1.4. Conceptos de fichero, tratamiento y cesión de datos. Ámbitos de tratamiento y cesión de datos personales del menor

Para poder aplicar la LOPD, se entiende necesaria la existencia de un fichero, conforme al art. 3 b) cualquiera que sea su soporte, pues si los datos no se incluyen en un fichero no es de obligado cumplimiento. Esta solución, se ampara en la idea de que solamente la información que se alberga de forma estructurada en un soporte puede ser tratada adecuadamente y, por ende, el interesado puede verse afectado en sus derechos por dichos tratamientos. A sensu contrario, una gestión aislada de un dato inconexo y desgajado de un conjunto ordenado no proporciona valor a dicha información ni erosiona los bienes jurídicos que la LOPD trata de proteger, de manera que no se justifica su activación. La definición de fichero viene de la mano de los arts. 5.1 K) RLOPD³² y 4.6) RGPD³³.

En lo que respecta al tratamiento de datos establece el art. 2.1 LOPD y RLOPD que son susceptibles de tratamiento cuando exista un conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Con lo cual, comprobamos que el concepto de tratamiento de datos es muy amplio y la mera captación de la imagen de una persona es un dato a tratar siempre y cuando sea mediante cámara fotográfica, videocámara, teléfono móvil o cualquier otro dispositivo que lo permita. Igualmente, el art. 4.2 RGPD hace una definición detallada del concepto de tratamiento de datos³⁴.

Para nuestro TC, tan solo con la recogida o grabación de datos personales existe tratamiento de datos aunque éstos no se conserven. El TJE en el ya citado caso Lindqvist enumera varios ejemplos de esas operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De este modo, la conducta que consiste en hacer referencia en una página web a datos personales debe considerarse un tratamiento de esta índole; pero quedará por determinar si dicho tratamiento está “*parcial o totalmente automatizado*”. Por lo tanto, difundir información en una página web implica, de acuerdo con los procedimientos técnicos e informáticos que se aplican actualmente, publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada. En definitiva, la conducta que consiste en hacer referencia en una página web a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un “*tratamiento total o parcialmente automatizado de datos personales*” conforme al art. 3.1 de la Directiva 95/46.

Ya en relación a la cesión o comunicación de datos, nuestro reglamento ha considerado que forma parte del tratamiento, no siendo necesaria una regulación específica y separada de esta operación, incluyéndola por ende en el régimen general del

³² Art. 5.1 K) “Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso”.

³³ Art. 4.4 “Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”.

³⁴ Art. 4.2 “Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción”.

tratamiento, si bien acompañada de algunas notas específicas. El art. 5.1 c) RLOPD dice que “*Tratamiento de datos supone su revelación a una persona distinta del interesado*”; y la única diferencia apreciable con la definición de la LOPD es su consideración explícita como “*tratamiento*”, lo que tampoco es necesario pues en la definición de este último concepto se incluyen, dentro del elenco de operaciones, las cesiones. Ahora bien, hay que tener en cuenta que la cesión es una operación que plantea problemas relacionados con la expansión o difusión de la información más allá del sujeto que originariamente la poseía, lo que conlleva la necesidad de mayores controles del flujo de datos y de trazabilidad de su circulación. Por ello, el peligro que implica la cesión de datos personales es variado: el conocimiento por múltiples personas, el control de quienes sean los destinatarios y la finalidad de los posteriores tratamientos, el mantenimiento en todo momento de la capacidad de decisión del interesado, a salvo las excepciones legales. Por otra parte, en el RGPD no se menciona la cesión de datos, pese a ello considero su inclusión en la definición de tratamiento al referirse a cualquier operación aunque no la recoja. Por el contrario, lo que sí introduce y define por primera vez son conceptos tales como “*violación de los datos personales*”, “*datos genéticos*”, “*datos biométricos*”, “*datos relativos a la salud*”, “*establecimiento principal*”, “*representante*”, “*empresa*”, “*grupo de empresas*”, “*normas corporativas vinculantes*” “*niño*” y “*autoridades de control*”.

Pese a lo anterior, MESSÍA DE LA CERDA BALLESTEROS³⁵, opina que quizás hubiera sido más conveniente mantener en el RLOPD una regulación de cesiones separada del tratamiento de datos, como lo demuestra el hecho de que gran parte de las resoluciones emitidas por los órganos de autocontrol continúen refiriéndose a tales actos de forma expresa. Es más, en el ámbito de la protección de los datos en Internet, la cesión o comunicación de los mismos constituye un aspecto fundamental de la protección, baste como ejemplo la inclusión de una definición y de una regulación específica sobre la comunicación de datos en la normativa de los EEUU sobre protección de la privacidad de los menores en Internet. Ya a nivel autonómico, la Ley 12/2008, de 3 de julio de protección integral de la infancia y la adolescencia de la Comunidad Valenciana ha mantenido dicha separación en contra de la normativa nacional

Por todo ello, constituye una cesión o comunicación de datos de carácter personal definida por el art. 3 j) LOPD “*Toda revelación de datos realizada a una persona distinta del interesado*” publicar fotos de los alumnos en la página web del colegio. En consecuencia, tanto la toma de las fotografías, como su publicación en Internet requieren el consentimiento del afectado o de sus padres si se trata de un menor de 14 años, de forma que cuando se tratan y ceden dichos datos personales sin el pertinente consentimiento, la LOPD establece el correspondiente mecanismo reactivo, cual es el derecho de cancelación de datos de carácter personal, recogido en su art. 16³⁶ tal como lo solicitó el padre respecto de la imagen de su hijo menor publicada en la página web en la Resolución de 10 de noviembre de 2009³⁷.

³⁵ MESSÍA DE LA CERDA BALLESTEROS J. A., “Algunas consideración sobre protección de datos personales de las personas menores de edad en Internet”, en *Los derechos de la personalidad de los menores y las nuevas Tecnologías*, (Coords. E. JORDÁ CAPITÁN y V. DE PRIEGO FERNÁNDEZ), El Derecho, Madrid, 2012, p. 114.

³⁶ Cabe señalar que el GT del Art. 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado art. de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en el Dictamen 2/2009, sobre la protección de los datos personales de los niños, en el que se contempla el especial supuesto de los colegios, recuerda, al referirse a los sitios web creados por éstos, que deben ser conscientes de que divulgar información personal justifica un cumplimiento más riguroso de los principios fundamentales de protección de datos. Igualmente recomienda que se pongan en marcha mecanismos de acceso restringido con vistas a proteger la información personal en cuestión, por ejemplo mediante la conexión con nombre de usuario y contraseña.

³⁷ R/02299/2009 (TD/00892/2009).

Tanto la AEPD como los Tribunales, han emitido diversas resoluciones de tratamiento de datos y de cesión de datos de menores sin el correspondiente consentimiento de los representantes legales. En tal sentido, se pueden clasificar diversos ámbitos de recogida de datos de los menores de edad:

-Las promociones o concursos dirigidos a menores: En las que deben cumplirse con los requisitos establecidos en el RLOPD para el tratamiento de datos de los menores de edad, incluso aunque se trate de ficheros temporales, lo que suele ser habitual cuando son promociones o concursos. Sirvan de ejemplo los supuestos que dieron lugar a la Resolución de 30 de noviembre de 2011³⁸, donde la empresa Panrico realizó una promoción a través de la web *www.toibollycao* en cuyas bases permitía la participación de menores, estableciéndose una opción para obtener el consentimiento de los representantes legales, pero al analizar los mecanismos de verificación de edad y obtención del consentimiento parental, lo cierto es, que la obtención de datos a través del formulario que debía enviarse en soporte papel no exigía en ningún momento el consentimiento de los representantes legales, por lo que claramente infringía las exigencias legales al respecto³⁹. La Resolución de 22 de diciembre de 2011⁴⁰ se trataba de un concurso para formar parte de una carroza en la Cabalgata de Reyes, promocionado por un canal infantil de televisión, en cuyo formulario que se cumplimentaba a través de una web, tan solo solicitaba datos de los menores sin que existiera ninguna opción para la autorización de los representantes legales⁴¹.

-Tratamientos de datos de menores por servicios de la sociedad de la información: Resultan interesantes por la utilización de servicios de videojuegos por los menores. La Resolución de 14 de marzo de 2008⁴² sancionó el sitio web por prestar diversos servicios para las personas que se registraran, entre ellos, trucos en el uso de videojuegos; además, los datos de registro nutrían un fichero que se utilizaba para realizar promociones comerciales, a pesar de que en los términos y condiciones de uso del servicio se señalaba claramente que su uso no estaba permitido a ese colectivo, un menor de 14 años consiguió registrarse en el sitio web recibiendo posteriormente una promoción comercial de un banco para la contratación de una tarjeta de crédito⁴³. La Resolución de 26 de abril de 2010⁴⁴ sancionó a un sitio web dirigido a un público infantil y juvenil que permitía, a los menores jugar y chatear entre otras actividades, por tratar datos de menores de 14 años sin consentimiento de sus representantes legales. La referida web recababa datos de usuario, contraseña y correo electrónico, pudiendo posteriormente, introducir la fecha de nacimiento, ciudad y país de procedencia; consecuentemente, la AEPD entendió que la dirección de correo electrónico (formada por el nombre e iniciales de los apellidos) asociada a la fecha de nacimiento permitía la identificación del titular, el cual, pudo darse de alta en la web sin consentimiento de los padres a pesar de constar que se trataba de un menor de 14 años. Por la publicación de imágenes de menores en Internet y Redes sociales, la Resolución 5 de marzo de 2009⁴⁵ se refiere a un caso de publicación en una

³⁸ R/02177/2011 (PS/00234/2011).

³⁹ La Sanción fue confirmada por la SAN 29/12/2012 (RJCA 2013, 99), aunque en el recurso la empresa pretendía que se imputara la responsabilidad únicamente a la empresa encargada del tratamiento con la que había contratado la realización de la promoción.

⁴⁰ R/02636/2011 (PS/00339/2011).

⁴¹ Otro caso de recogida de datos para participar en un concurso es la Resolución de 5 de octubre de 2009 (R/01974/2009 (PS/00293/2009), si bien se sancionó por la falta de cumplimiento del deber de informar, pues se había recabado datos de menores de edad a través de un cupón para participar en un sorteo contenido en una conocida revista dirigido a un público sobre todo menor de edad.

⁴² R/00284/2008 (PS/00281/2007).

⁴³ Las sanciones impuestas a la entidad en esta Resolución fueron confirmadas por la SAN 26/11/2009 (JUR 2009, 496350).

⁴⁴ R/00893/2010 (PS/00468/2009).

⁴⁵ E/00989/2008.

web de datos de menores de edad (dirección IP de los internautas, entre ellos, menores de edad), aunque fue archivado al no poder establecerse quién era el responsable del sitio web; y la Resolución de 30 de julio de 2010⁴⁶ sancionó a un portal de Internet especializado en establecer contactos personales entre usuarios jóvenes o adolescentes a través de mensajes interactivos, y ello, por contener perfiles de menores de 14 años y tratar sus datos sin consentimiento de sus representantes legales. En concreto, el sitio web recababa a través de un formulario de registro los datos de nombre de usuario, contraseña, correo electrónico, sexo, fecha de nacimiento (anterior a 1 de enero de 1994), país, provincia y fotografía (registro que debía ser validado antes de hacerse público). Se pudo constatar, que ningún usuario registrado tenía declarada una edad menor de 15 años (edad mínima), buena parte de las fotografías parecían corresponder a menores de 14 años en actitudes provocativas y exhibicionistas. Además, junto a los comentarios y fotografías, se incluían banners publicitarios que permitían acceder a otros sitios web desde los que se facilitaba la suscripción a servicios SMS-Premium (cartas astrales, concursos...), información comercial sobre videojuegos, otras páginas de contactos, etc.

-Tratamiento de la imagen de los menores de edad en centros educativos:

Reviste especial interés las Resoluciones de 15 de julio de 2008⁴⁷ que sancionan la cesión de datos de los alumnos de una escuela primaria a una editorial para realizar una publicación sobre el centro, sin que se hubiera solicitado el consentimiento de algunos representantes legales; la Resolución de 16 de noviembre de 2009⁴⁸ que también sanciona a una federación deportiva por publicar en su web los resultados de competiciones de menores sin consentimiento de los padres; la Resolución de 5 de noviembre de 2010⁴⁹ por sancionar a un colegio, si bien en este caso revela datos de un menor de edad (art. 10 LOPD) (nombre, condición de alumno del centro y estudios que cursaba) a los padres de otro menor del centro. Otros casos similares son la Resolución de 24 de febrero de 2011⁵⁰ por la fotografía de un alumno de una escuela de música tomada durante un festival de curso, la cual fue utilizada en los folletos publicitarios de la escuela, sin el consentimiento de los representantes legales. En la Resolución de 1 de octubre de 2015⁵¹ se sanciona al Colegio Ecole por publicar fotografías sin el consentimiento de una alumna menor ni de sus padres, en la página web del colegio, su perfil de Facebook y su blog, así como en Youtube. Con la Resolución de 2 de noviembre de 2015⁵² se apercibe (previa a la sanción al Colegio) para que dejen de aparecer en su revista imágenes del hijo menor discapacitado sin el consentimiento del menor ni de sus padres o tutores legales. Una situación cada vez más extendida es la captación o tratamiento de datos personales a través de videocámaras en entornos escolares en cuyo caso también se les aplicaría los principios en materia de protección de datos pero sin olvidarse en particular del principio de proporcionalidad al tratarse de menores de edad⁵³. En este sentido, se debe tener en cuenta la Instrucción 1/2006, de 12 de diciembre de la AEPD sobre el tratamiento con fines de vigilancia a través de sistemas de cámaras o videocámaras; de tal manera, que para la AEPD sólo deben instalarse cuando se considere insustituible, resulte una medida adecuada al fin que se pretende conseguir y no exista otra menos invasiva en los derechos

⁴⁶ R/01663/2010 (PS/00023/2010).

⁴⁷ R/00905/2008 (PS/00499/2007) y R/00914/2008 (AP/00003/2008).

⁴⁸ R/02285/2009 (PS/00010/2009).

⁴⁹ R/02162/2010 (PS/00225/2010).

⁵⁰ R/00330/2011 (PS/00477/2010).

⁵¹ PS-00214-2015. Resolución de 1 de octubre de 2015 de la AEPD.

⁵² A-00145-2015. Resolución de 2 de noviembre de 2015 de la AEPD.

⁵³ Vid. Informe 274/2009 y la Guía de Video vigilancia 2009 de la AEPD accesible en la página web de la Agencia: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf.

de los menores⁵⁴, pero con una serie de limitaciones en cuanto al lugar o periodos en los que se puede tomar la imagen, para no colisionar con los derechos a la intimidad y a la libertad de enseñanza⁵⁵. Por eso, la AEPD diferencia entre captar imágenes con fines de seguridad o no. En el primer caso, la Ley 23/1992, de 30 de julio, de Seguridad Privada legitimaría para el tratamiento de imágenes sin la necesidad de contar con el consentimiento de las personas afectadas; sin embargo, en el segundo caso sería necesario tener el correspondiente consentimiento para su tratamiento⁵⁶.

-Tratamiento de los datos personales de los menores de edad al contratar o modificar las condiciones de la contratación realizadas con la operadora telefónica:

Al respecto, cabe citar la Resolución de 11 de noviembre de 2008⁵⁷ que sancionó a la empresa Telefónica Móviles España al acreditarse la adquisición de un pack telefónico (con línea de prepago) y la emisión de una factura a un menor de 13 años sin el consentimiento de sus representantes legales. Las Resoluciones de 11 de noviembre de 2008⁵⁸ y 22 de noviembre de 2008⁵⁹ sancionaron a la empresa Telefónica por contratar con menores el cambio de la línea de teléfono de prepago a contrato (en el primer caso, un menor de 17 años y en el segundo, una menor de 13 años); y la Resolución de 19 de agosto de 2009⁶⁰ sancionó a la empresa Telefónica por la contratación de un menor de 14 años de una línea de teléfono, si bien fue anulada por la SAN 1 de abril de 2011⁶¹ por considerar que existía consentimiento del representante legal del menor. Ahora bien, en línea con el CC, jurisprudencia⁶² y la AEPD⁶³, LUQUIN BERGARECHE considera que adquirir un terminal telefónico y/o la contratación de una línea telefónica (en particular, mediante la modalidad de pos pago), no se pueden calificar contratos de escasa entidad acordes a la madurez del menor ya que pueden suponer el desembolso de importantes cantidades de dinero a través de las facturas que se genere. El criterio de la AEPD es establecer como regla general que un menor no emancipado no tiene capacidad para contratar, y en consecuencia, tampoco para consentir por sí solo el tratamiento de datos derivado de dicho contrato, y ello, con independencia de que se supere la edad de los 14 años establecida en el art. 13 RLOPD⁶⁴. Por consiguiente, cuando el tratamiento de datos pueda tener consecuencias en su esfera patrimonial, el límite de 14 años será desplazado requiriéndose la autorización o convalidación de los representantes legales; en cambio, en los supuestos previstos en el art. 164.3 CC, que permite al menor mayor de 16 años realizar actos de administración ordinaria respecto de los bienes adquiridos con su trabajo

⁵⁴ Para la AEPD (Guía de Video vigilancia, p. 25), la instalación de cámaras de vídeo vigilancia sería una medida proporcional y justificada si se cumplen los siguientes requisitos: a) que se trate de una medida susceptible de conseguir el objetivo propuesto; b) que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia; c) que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

⁵⁵ No puede existir vídeo vigilancia en lugares como baños, vestuarios o gimnasios y su uso en aulas o zonas de recreo debe ser excepcional tampoco se puede captar imágenes con fines de control escolar. Vid. el Informe 345/2009, cuyo tema es la instalación de cámaras por razones de seguridad en un colegio.

⁵⁶ Guía vídeo vigilancia, p. 37.

⁵⁷ R/01349/2008 (PS/00315/2008).

⁵⁸ R/01405/2008 (PS/00316/2008). En cambio, la SAN 10/2/2010 (JUR 2010,82779) que resolvió el recurso contra dicha resolución, lo anula, no tanto porque considere que el menor tiene capacidad para contratar, sino basándose en la capacidad para consentir el tratamiento de datos en base al art. 13 RLOPD.

⁵⁹ R/01359/2008 (PS/00330/2008).

⁶⁰ R/01891/2009 (PS/00088/2009).

⁶¹ JUR 2011, 135060.

⁶² SAN 25/3/2010 (JUR 2010, 124010) resuelve el recurso contra la Resolución de 11 de noviembre de 2008 y considera que no cabe encuadrar dicho contrato en el art. 162 CC, teniendo en cuenta la edad del menor y las características de la adquisición mediante pago con tarjeta.

⁶³ R/01349/2008 (PS/00316/2008).

⁶⁴ ANDREU MARTÍNEZ, M.B., *La protección de los datos personales de los menores de edad*, Thomson-Reuters Aranzadi, Navarra, 2013, p.114.

o industria, o cuando se trate de un menor emancipado sí podría admitirse tal capacidad⁶⁵. Sin embargo, en contra del criterio de unidad en la capacidad para contratar y consentir el tratamiento de datos personales de la AEPD, nuestra jurisprudencia española, desvincula tal unidad, es decir, por una parte está la capacidad para contratar que se rige conforme a las normas del CC y por otra, la capacidad para consentir el tratamiento de sus datos personales que se le aplica el art. 13 RLOPD⁶⁶. Por ello, en tanto en cuanto no exista una norma que expresamente establezca la necesidad de intervención de los representantes legales para el tratamiento de datos no se puede acudir al precepto que regula la capacidad de obrar del menor en relación a otra cuestión de la que deriva el tratamiento de datos. La AN, no entra a valorar la capacidad del menor para contratar, tan solo dilucida la cuestión del tratamiento de datos personales desvinculado del acto material del que deriva. Comparto con la autora ANDREU MARTÍNEZ⁶⁷ el rechazo a tal postura al desvincular de forma más que criticable la normativa de protección de datos de otras normas sobre la capacidad de los menores existentes en el ordenamiento jurídico y convertir al citado art. 13 en una regla aislada e impermeable en materia de protección de datos personales⁶⁸.

- La inclusión en Ficheros morosos de los datos personales de los menores de edad como consecuencia del incumplimiento del contrato: A título de ejemplo, la SAN de 29 de abril de 2005⁶⁹ se ha pronunciado en una titularidad de una cuenta corriente bancaria para parte de un menor y la posibilidad de su inclusión en un fichero de morosos por el saldo deudor resultante y concluye que como cotitular de una cuenta bancaria puede ser deudor e incurrir en la condición de moroso, aunque sea su madre (en su condición de representante legal) quien actuara por él⁷⁰. En la citada sentencia se fijan los criterios que se siguen en resoluciones posteriores, incluidas las de la propia AEPD como la Resolución de 27 de abril de 2009⁷¹ que también trata de un caso de cotitularidad por parte de una menor de una cuenta corriente e inclusión de sus datos en fichero de morosos por saldo deudor. Otro caso, es el resuelto en la SAN de 1 de abril de 2011⁷², en el cual una madre (ante la imposibilidad de realizarlo a su nombre), contrató una línea telefónica en nombre de su hijo de 14 años domiciliando los recibos en una cuenta de su titularidad, ante el impago de algunos recibos, los datos del menor (y únicamente los de éste) fueron incluidos en un fichero de morosos siendo denunciado por la madre. Podría plantearse la cuestión de si la inclusión de los datos de un menor en un fichero de morosos lesiona su derecho a la intimidad, tal y como el Fiscal de menores del Tribunal Superior de Justicia (TSJ) de Asturias alegó en la mencionada SAN 29 de abril de 2005; pues bien, el tribunal considera que es inaplicable el art. 4 LOPJM al ámbito que nos ocupa y para ello se basa

⁶⁵ LUQUIN BERGARECHE, R., *La protección Jurídico-Civil del Menor Usuario de Telefonía Móvil en la Sociedad de la Tecnología*, mantiene que a diferencia de los supuestos de emancipación (art. 1263.1 CC), los menores no emancipados no pueden prestar un consentimiento contractual válido y eficaz en estos casos, incluso aunque se trate de la adquisición de una tarjeta de crédito. Analiza, además, los diferentes casos de contratación en el caso de menores no emancipados que se suelen dar en la práctica por los representantes legales o por los propios menores (así, contratación de servicios de telefonía móvil por los representantes legales en su propio nombre o en nombre del menor cediendo el uso a éste; contratación por el menor de edad en su propio nombre, a veces a través del terminal adquirido por él mismo en modalidad de prepago-dentro de un gasto módico- y la contratación de los servicios por parte de los menores a través de terminal adquirido por los representantes legales en modalidad de prepago). Cuadernos de Aranzadi civil, Navarra, 2012, pp.69, 81 y ss.

⁶⁶ En ese sentido, citar las SSAN 14/1/2009 (JUR 2009, 59625) y 10/2/2010 (JUR 2010, 82779).

⁶⁷ ANDREU MARTÍNEZ, ob. cit., p. 116.

⁶⁸ Conforme al art. 1.301CC, la consecuencia de la contratación de un menor sin consentimiento del representante legal como regla general es la anulabilidad del contrato, en cambio para la AEPD cuando sea menor de 14 años es la nulidad absoluta pese a no existir base legal alguna en la que se pueda sustentar.

⁶⁹ JUR 2005, 264576.

⁷⁰ LÓPEZ SÁNCHEZ C., *La responsabilidad civil del menor*, Dykinson, Madrid, 2001, pp. 247 y ss.

⁷¹ E/00297/2007.

⁷² JUR 2011, 130560.

en que no se puede equiparar tal inclusión que tiene un ámbito restringido de difusión con la difusión de los medios de comunicación a los cuales se refiere el citado precepto; en cualquier caso, no se debe olvidar que la intimidad del menor quedaría siempre protegida por la LOPDH.

2.1.5. El deber de informar la recogida y el tratamiento de los datos personales del menor

Con carácter general y previo a consentir es muy importante que las redes sociales cumplan con el principio de información recogido en el art. 5 LOPD⁷³, de manera que, el titular de los datos ya sea mayor o menor debe ser previamente informado en primer lugar de la existencia de un fichero y de un tratamiento con sus datos personales; en segundo lugar, del carácter obligatorio o facultativo de la respuesta; en tercer lugar, de las consecuencias de obtención de los datos y de la negativa a suministrarlos; en cuarto lugar, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (ARCO); y en último lugar, de la identidad, dirección postal y electrónica del responsable del fichero y del servicio para el ejercicio de los derechos ARCO. En la nueva LOPD se regulan en sus arts. 13, 14, 15, 16, 17 y 18 y concretamente se denominan los derechos de acceso, de rectificación, de supresión (derecho al olvido), a la limitación del tratamiento, a la portabilidad y de oposición).

Por ello, es necesario que se lea y se acepte expresamente la política de privacidad antes de la publicación del perfil con datos personales en la red social, por lo que no debe ser posible la introducción de ningún dato sin que el afectado haya dado su consentimiento expreso, en el que acepte los términos y condiciones de la política de privacidad de la red social. Pese a lo anterior, no todas las redes sociales cumplen la normativa de protección de datos personales en este punto, ya que la política de privacidad no está destacada suficientemente en las páginas de inicio y en la fase de registro⁷⁴. Consecuentemente, no existe un conocimiento de quién posee sus datos, para qué finalidad, ni se conocen de manera completa las posibles cesiones y el almacenamiento de cookies, y aunque existe una apariencia de consentimiento, el incumplimiento del principio de la información implica que no existe un consentimiento informado.

El nuevo RGPD, trata esta cuestión al introducir el principio de transparencia de la información y comunicación en relación con el usuario (art. 5.1. a) lo que tiene consecuencias para los servicios de redes sociales en relación con la información y, con el derecho de acceso, ya que la información al interesado deberá incluir no sólo los fines del tratamiento sino también el interés legítimo del responsable, información sobre el plazo dentro del cual se conservarán los datos (ya recogido en la LOPD), el derecho a presentar una reclamación ante la autoridad de control, y en su caso, la intención del responsable de efectuar una transparencia internacional y el nivel de protección del tercer

⁷³ Art.5.1 “Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.

⁷⁴ Muy pocas personas leen la política de privacidad -donde se señala la explotación de la información por intereses económicos- especialmente los jóvenes. Hay que destacar que los digitales nativos son objeto de un interés específico por las compañías de publicidad.

país⁷⁵. Asimismo, en el art. 11 PLOPD tal principio se convierte en un derecho de transparencia e información que tienen las personas.

En relación al menor, para el caso de que pueda prestar por sí mismo consentimiento para el tratamiento de sus datos personales, primero debe conocer exactamente que está consintiendo con lo que la información previa y detallada es una condición indispensable para el otorgamiento de un consentimiento válido. Teniendo en cuenta que donde los menores ceden sus datos es sobre todo en Internet, conviene prestar atención al modo en que los prestadores de servicios recaban el consentimiento de los usuarios al solicitarles determinados datos de carácter personal. Normalmente, la práctica más extendida para cumplir este requisito legal es la inserción de un aviso legal en las páginas web y en los formularios de recogida de datos. El problema es que por lo general, la redacción de dichos avisos legales es bastante técnica y aunque cumple formalmente con el texto de la LOPD, no es una información útil para el menor de edad al no entender plenamente su contenido. Por eso, la doctrina ha remarcado la importancia de que la redacción de los avisos legales que presumiblemente van dirigidos a menores de edad tenga en cuenta el nivel de educación de éstos, empleando un tenor comprensible del menor⁷⁶.

Ahora bien, respecto a aquellos menores que tengan capacidad de discernimiento suficiente pero que no puedan prestar aún el consentimiento, ¿pueden ser también destinatarios de la información relativa al tratamiento de sus datos personales, aunque presten el consentimiento sus representantes legales? GÓMEZ-JUÁREZ SIDERA⁷⁷ defiende que se informe tanto a los representantes legales como al menor, en contra PRATS ALBENTOSA⁷⁸ entiende que en el caso de menores de 14 años la relación se establecerá entre el responsable y los representantes legales, que son quienes han de consentir. Por mi parte, considero que sí tienen derecho a recibir información necesaria para su desarrollo y a participar en las decisiones que les afecten desde que tenga suficiente juicio, aunque consientan los representantes legales; sobre todo, en los sitios web dirigidos específicamente a menores pues con independencia de que la información la dirijan a los representantes legales y sean éstos quienes consientan en el tratamiento de datos, deberán tener adaptada la información relativa al tratamiento de datos a las capacidades de entendimiento de un menor⁷⁹.

No nos debemos olvidar, que el incumplimiento del deber de información conforme al art. 5 LOPD (art. 11 RLOPD) supone una infracción de la normativa de protección de datos que puede conllevar importantes sanciones como por ejemplo en el caso de la Resolución de la AEPD de 5 de octubre de 2009⁸⁰ donde se sancionó en 6.000 euros a la empresa Panini por recabar datos personales de menores para participar en un sorteo a través de cupones en la revista *High School Musical* por incumplimiento de la información del art. 5 LOPD. En la nueva LOPD tal incumplimiento se califica como una infracción leve conforme al art. 74.a).

⁷⁵ TRONCOSO REIGADA, ob. cit., pp. 73-74.

⁷⁶ GÓMEZ-JUÁREZ SIDERA, I., *La protección de los datos del menor como e-consumidor. Consumidores y usuarios ante las nuevas tecnologías*, (Coord. L. COTINO HUESO), Tirant lo Blanch, Valencia, 2008, p. 718.

⁷⁷ GÓMEZ-JUÁREZ SIDERA, ob. cit., pp. 718 y ss.

⁷⁸ PRATS ALBENTOSA, L., "Principios de protección de datos: Calidad de los datos, consentimiento para el tratamiento de datos y deber de información" en *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (aprobado por RD 1720/2007, de 21 de diciembre)*, (Dirs. A. PALOMAR OLMEDA y P. GONZÁLEZ-ESPEJO), Thomson-Civitas, Cizur Menor, Navarra, 2008, p. 177.

⁷⁹ Cabe hacer referencia de nuevo a la SAN 29/12/2012 (RJCA 2013,99) que sanciona a la empresa como consecuencia de incumplir con la obligación de informar "necesaria diligencia en el tratamiento de los datos y la información a suministrar a menores de 14 años".

⁸⁰ R/01974/2009 (PS/00293/2009).

A mi juicio, la línea en la que se debe avanzar es la necesidad de concienciar a los prestadores de servicios de la necesidad de dar una información adaptada a las capacidades de entendimiento de los menores, pues solo así, se puede garantizar el cumplimiento de este deber⁸¹.

2.1.6. El consentimiento del menor en el tratamiento de sus datos personales

En lo atinente al consentimiento de los usuarios, lo primero que debemos tener en cuenta es que proporcionan datos personales para generar su descripción o perfil y con ellos el proveedor de un servicio de redes sociales lleva a cabo un tratamiento de los mismos. Ahora bien, para tratar los datos de carácter personal se requerirá el consentimiento inequívoco del afectado salvo que la ley disponga otra cosa. Y ese consentimiento, debe ser una manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernen.

La AEPD entiende por “consentimiento libre”, aquel que haya sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el CC; “específico”, se refiere a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento; “inequívoco” se exige la realización de una acción u omisión que implique la existencia del consentimiento e “informado”, cuando el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se produce⁸².

Cabe decir, que en materia de protección de datos se admite el consentimiento expreso y tácito⁸³; de tal modo, que este último existe cuando el tratamiento de datos no afecte a datos especialmente protegidos (art. 7.2 y 3 LOPD) y está regulado detalladamente en el art. 14.2 del RLOPD. En este sentido, la AEPD en su Dictamen 93/2008⁸⁴, se ha pronunciado sobre las formas de prestar el consentimiento mediante webs, analizando entre ellos el consentimiento tácito. Sin embargo, en la nueva LOPD ya no cabe el consentimiento tácito y además se establece la obligación de requerir el consentimiento específico para cada una de las finalidades, no siendo viable por tanto para el tratamiento de datos un consentimiento genérico tal como establece el art. 6⁸⁵.

⁸¹ Vid. Informe 308/2008 de la AEPD, en el que se señala la obligación de cumplir con el deber de informar al menor conforme al art. 13.3 RLOPD para que su consentimiento sea válido. Y el Informe 46/2010, destaca mayor rigor en el deber de informar cuando el destinatario sea un menor de edad.

⁸² Informe jurídico emitido por la AEPD, 0917/2013, referido en uno de sus puntos a la regulación existente en la LOPD y en el RLOPD en relación al consentimiento de los usuarios.

⁸³ Respecto al consentimiento presunto, vid. Artículo “El consentimiento presunto no es válido en protección de datos salvo para CCOO” de D. GONZÁLEZ CALLEJA: <http://descargalegal.blogs.lexnova.es/2011/12/05/el-consentimiento-presunto-no-es-valido-en-protección-de-datos-excepto-para-ccoo/>.

⁸⁴ “En el supuesto de que la recogida de datos se realice a través de una página web, las obligaciones a las que acabamos de referirnos, suelen cumplirse mediante formularios y cláusulas a los que se accede a través de enlaces como pueden ser “aviso legal” o “política de protección”. También es importante incluir algún tipo de “link” de este tipo en relación con los derechos de los interesados de rectificación, cancelación, acceso y oposición. En cuanto al consentimiento informado, este habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia.

⁸⁵ Art. 6. “Tratamiento basado en el consentimiento del afectado. 1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas. 3. No podrá supeditarse la ejecución del contrato a que

Pero como se puede observar, la LOPD nada dice en cuanto al consentimiento para el tratamiento de datos de los menores de edad, únicamente establece en el art. 13 del RLOPD, un límite expreso cual es la edad de 14 años para que el consentimiento prestado por un menor en la utilización de sus datos personales sea válido. El apartado uno del citado precepto⁸⁶, diferencia dos categorías de menores de edad, situando la edad de 14 años, como la frontera para consentir el menor el tratamiento de sus datos en ficheros automatizados; de manera que, cuando son mayores de 14 años “*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela*”⁸⁷. Con ello, se deja claro que la capacidad para consentir el tratamiento de sus datos personales no se adquiere antes de los 14 años⁸⁸, pues se presupone que a los 14 años se tiene ya unas condiciones de madurez suficiente para consentir por sí mismos en que se traten sus datos de carácter personal, incluidos los sensibles, al no existir distinción alguna en el citado precepto, lo cual no deja de plantear dudas sobre todo en ciertos ámbitos (por ejemplo marketing directo)⁸⁹. Por el contrario, cuando son menores de 14 años “*Se requerirá el consentimiento de los padres o tutores*” para lo cual, toma como referencia la normativa civil, en la que el menor no reúne las condiciones de madurez suficientes, ni dispone de capacidad para la celebración de determinados actos civiles como puede ser el otorgar el consentimiento para el tratamiento de sus datos personales.

A pesar de todo, este apartado establece una presunción general de madurez a los 14 años para el tratamiento de sus datos personales en base al criterio fijado por la AEPD en su Memoria 2000, donde interpreta el citado precepto en conjunto con otras normas, y toma como referencia a los mayores de 14 años por considerar que disponen de las condiciones de madurez suficiente para consentir acerca del tratamiento de sus datos, “*Toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los*

el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”.

⁸⁶ Esta capacidad de los mayores de catorce años para prestar su consentimiento al tratamiento de datos personales fue anticipada por la Memoria 2000, Agencia Española de Protección de Datos, Madrid, 2001, pp. 381 y ss. En lo que a los menores de catorce años respecta, la Memoria dejaba la cuestión del consentimiento a sus condiciones de madurez suficiente, sin especificar quién determina si el menor reúne dichas condiciones. Esta laguna ha sido cubierta con el art. 13 del RLOPD.

⁸⁷ TRONCOSO REIGADA, A., “La protección de los datos sanitarios del menor”, en *Nuevos retos que plantean los menores en Derecho. III Jornadas sobre Derecho de los menores*, (Coords. I. E. LÁZARO GONZÁLEZ e I. V. MAYORAL NARROS), Publicaciones de la Universidad Pontificia de Comillas, Madrid, 2004, pp.213 y ss. En el ámbito médico, el menor no puede consentir por sí solo el tratamiento de los datos médicos en el caso de un determinado acto médico como por ejemplo una operación quirúrgica. Vid. Informe 466/2004 y las Resoluciones de 11 de noviembre de 2008 (R/01405/2008, PS/00316/2008) y 19 de agosto de 2009 (R/01891/2009, PS/00088/2009). Para GRIMALT SERVERA, P., “Los menores en internet: capacidad *versus* protección de la vida privada” en *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, (Coords. M. CUENA CASAS, L. A. ANGUITA VILLANUEVA y J. ORTEGA DOMÉNECH), Dykinson, Madrid, 2013, pp. 187 y ss. Igualmente excluye la capacidad para contratar a los menores no emancipados (art. 1263.1 CC), previsión también aplicable en el caso de datos íntimos o la propia imagen, en los que habrá que atender a las condiciones de madurez para prestar el consentimiento por parte de los menores previstas en el CC y la LOPDH y no el art. 13.1 RLOPD. Pese a que nuestra jurisprudencia no sigue este criterio, pues exige la existencia de una norma que expresamente establezca la necesidad de intervención de los representantes legales para el tratamiento de datos personales no siendo suficiente la norma que establezca la necesidad de los representantes legales para contratar.

⁸⁸ Así lo afirma expresamente la AEPD en su Informe jurídico 308/2008, para el caso de SMS recibidos por un menor en su teléfono móvil. También el Informe 179/2010, sobre la necesidad de contar con el consentimiento de los representantes legales para la creación de direcciones de correo electrónico a menores de un centro escolar cuando intervenga un prestador de servicios de la sociedad de la información. Previsión seguida por la AEPD que entiende que el tratamiento de datos personales de menores debe estar en relación con la capacidad contractual de éstos.

⁸⁹ Duda OROZCO PARDO, G., “Intimidad, privacidad, “extimidad” y protección de datos del menor. ¿Un cambio de paradigma? “en *La Protección Jurídica de la intimidad*, (Dir. J. BOIX REIG y Coord. A. JAREÑO LEAL), Iustel, Madrid, 2010, p. 401, que el art. 13 RLOPD habilite para recabar datos sensibles.

mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solo determinados actos de la vida civil”⁹⁰; para llegar a tal conclusión, ha partido del art. 162.2.1 CC y se ha apoyado en determinados actos de la vida civil en los cuales se reconoce a los mayores de 14 años capacidad de discernir y madurez suficiente para realizarlos por sí solos tales como adquirir la nacionalidad española o testar; de tal manera, que ha abogado por conjugar la edad, como presunción iuris tantum con la capacidad natural y madurez del menor. En cambio, con respecto a los menores de 14 años, la AEPD, tan solo señala vagamente que “No puede ofrecerse ninguna solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el art. 162.1º CC, teniendo en cuenta, fundamentalmente sus condiciones de madurez”, pese a referirse al criterio de la madurez, en cierto modo, los obvia y requiere el consentimiento de los padres o tutores.

Algunos autores cuestionan si el menor goza de la capacidad jurídica suficiente para consentir sobre el tratamiento de sus datos⁹¹. Y así, TRONCOSO REIGADA⁹² considera que se debe estar a cada caso, especialmente, en los distintos tramos de edad. CASTELLÓ MARTÍNEZ⁹³ añade que la edad mínima para participar es objeto de amplio debate en el ámbito de las redes sociales on line, pues una vez leídas y aceptadas las condiciones de contratación y prestado el consentimiento, la persona queda registrada como usuario. ABA CATOIRA⁹⁴ se pregunta cómo es posible aplicar la norma del art. 13 ROLPD si muchas veces son los propios menores de 14 años, quienes se registran en las redes sociales sin haber alcanzado aún plena madurez ni responsabilidad. Por su parte, LUQUIN BERGARECHE⁹⁵ critica la edad de 14 años fijada en el citado reglamento, pues entiende que un preadolescente de 14 años no está suficientemente preparado para consentir el tratamiento de sus datos personales en ficheros y registros automatizados de datos, con las consecuencias que ello puede acarrear; sin embargo, con el fin de otorgar mayor seguridad jurídica en la red, la gran mayoría de la doctrina piensa que el citado apartado viene a clarificar y dar solución a una cuestión que no estaba del todo resuelta en las normas precedentes, pues se ha decantado por fijar una frontera en materia de la edad de los menores y su capacidad para consentir en materia de cesión de datos personales siendo un elemento de más fácil comprobación para permitir el acceso a la red. No obstante, tal y como oportunamente señala BARTOLOMÉ TUTOR⁹⁶ son cuestiones distintas una, el acceso a la red y, otra, que una vez que hayan accedido sus actuaciones pongan en situación de vulnerabilidad su intimidad, honor, imagen e incluso la protección de sus propios datos personales, en donde habría que jugar con parámetros de madurez, en tanto ésta permitirá que el menor sea capaz de barajar si consiente o no una intromisión ilegítima en estos derechos propios de la esfera privada. Comparto la

⁹⁰ MEMORIA 2000 de la AEPD, ob. cit., pp. 381 y ss.

⁹¹ GÓMEZ-JUÁREZ SIDERA, afirma que dado el carácter transnacional de la Red, resulta problemática la diversidad de criterio a la hora de establecer una edad de protección reforzada para el tratamiento de datos en los diferentes países. En España la edad está fijada en catorce años; en EEUU, en trece; el llamado Grupo de Berlín, (foro internacional que aglutina autoridades de protección de datos de muchos países), ha trabajado también con la edad de dieciséis años. Ob. cit., p. 720.

⁹² TRONCOSO REIGADA, ob. cit., p. 1231.

⁹³ CASTELLÓ MARTÍNEZ, A., “Ética en publicidad Online”, Fonseca, *Journal of Communication*, nº 1, ISSN: 2172-9077, p. 232.

⁹⁴ ABA CATOIRA, A., “Los menores ante Internet: las redes sociales”, www.js-e.cat/site/arxius/pdfs/Ana-_M-Aba-Catoira-PONENCIAS.pdf, p. 16.

⁹⁵ LUQUIN BERGARECHE, ob. cit., p. 201.

⁹⁶ BARTOLOMÉ TUTOR, A., *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, Thomson-Reuters Aranzadi, Navarra, 2015, p. 287.

opinión con GIL ANTÓN⁹⁷ que la prestación del consentimiento por el menor no debiera ser fijado únicamente en función del dato objetivo de la edad y el criterio subjetivo de la suficiente madurez, sino que además, debería tenerse en cuenta la formación o información o de ambas, pues los datos que se vuelcan en la red producen “*una cesión de datos en un lugar que el menor de 14 años no sabe cómo realmente funciona*”, esto es, el menor desconoce si en donde cede los datos existe algún tipo de indexación por otras páginas, u otros elementos, por ello debería tener una adecuada formación al respecto. El problema está en su acreditación y como se procedería a la valoración y ponderación en su caso; no obstante, también se ha cuestionado la constitucionalidad de que un RD limite para un colectivo -los menores de edad- un derecho fundamental. En ese sentido, coincido con VÁZQUEZ DE CASTRO⁹⁸ y MARTÍNEZ OTERO, que hubiera sido más oportuno que una restricción de este tipo fuera recogida en una norma con rango de LO, toda vez que hubiese surgido del poder legislativo con una mayoría reforzada.

De todo lo mencionado, cabe resaltar que el derecho del menor interesado en prestar su consentimiento por sí o por medio de sus representantes, para el tratamiento de sus datos personales es la garantía y el instrumento principal para todos, y así lo recoge la propia Carta de Derechos Fundamentales de la Unión Europea en su art. 8.1 cuando dice que “*El tratamiento de los datos personales solo es posible previo consentimiento del afectado*”. En igual línea, se decantaba la Propuesta del Reglamento, si bien rebajaba el límite a la edad de 13 años para la obtención de ese consentimiento, exigiendo el consentimiento de padres y tutores para los menores de 13 años y debiendo ser dicho consentimiento prestado para posibilitar el tratamiento de datos personales en la red, expreso y verificable. Sin embargo, el RGPD eleva la edad para consentir el menor a partir de los 16 años, dando libertad a los estados miembros para que establezcan otra edad la cual en ningún caso puede ser inferior a los 13 años. Esta última matización conlleva la posibilidad de mantener la edad límite de 14 años recogida en la normativa española o elevarla hasta los 16 años. Finalmente, el PLOPD con el fin de ajustarse al citado Reglamento europeo y unificar la edad con los miembros de la Unión Europea ha optado por rebajar a 13 años el consentimiento de los menores tal como recoge su art. 7⁹⁹. Asimismo, en la nueva LOPD, conforme a su art. 63 se establece un régimen jurídico específico que se remite a lo dispuesto en el nuevo RGPD, a la presente ley, a las disposiciones reglamentarias que se desarrollen y a las normas generales sobre procedimientos administrativos cuando no contradigan a los anteriores. En este sentido, el nuevo RGPD regula en su art. 79 el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento¹⁰⁰ e introduce una nueva

⁹⁷ GIL ANTÓN, A. M., *El derecho a la propia imagen del menor en Internet*, Dykinson, Madrid, 2013, p. 196.

⁹⁸ VÁZQUEZ DE CASTRO, se cuestiona también la idoneidad de una norma de rango reglamentario para fijar esta frontera de edad, y propone su incorporación al articulado de la LOPD. VÁZQUEZ DE CASTRO, E., “Protección de datos personales, redes sociales y menores”, *Revista de Aranzadi de Derecho y Nuevas Tecnologías*, nº 29, 2012, pp. 54-58.

⁹⁹ Art. 7. “Consentimiento de los menores de edad. 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de trece años sólo será lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela”.

¹⁰⁰ Art. 79 RGPD “1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales. 2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales

regulación del “Derecho a indemnización y responsabilidad” en su art. 82, de manera que prevé como habitual las reclamaciones de daños y perjuicios por daños identificables y cuantificables en caso de sanción por vulnerar dicha norma, y así, en su apartado 1 dice que *“Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos”*.

Otro aspecto que se debe poner de relieve, es la diferencia existente sobre la actuación de los responsables parentales según sea el derecho al honor, intimidad e imagen o el derecho a la protección de datos. Mientras que en la normativa sobre protección al honor, intimidad e imagen se refiere constantemente a la intervención de los representantes legales, pese a que como cree BARTOLOMÉ TUTOR¹⁰¹ debería hablarse de titulares de la patria potestad en calidad de asistentes, tal como lo recoge el actual art. 162. 1 CC, modificado por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia (LMSPIA). En cambio, el RLOPD incorpora a los responsables parentales no como representantes legales, sino que de su redacción se puede inferir esta actuación dentro de los deberes de asistencia y cuidado, conforme al art. 154 CC.

En cuanto al apartado dos, se detalla qué tipo de datos son los que no se pueden solicitar del menor, siendo por tanto condición sine qua non que *“Cualquier responsable de fichero obtenga el consentimiento expreso cuando sea un mayor de 14 años y por escrito de sus padres o tutores cuando sea un menor de 14 años y afecte a terceras personas del entorno familiar”* y *“los que se pueden solicitar y su finalidad”*. De tal forma, que *“En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior”*. Por lo tanto, el consentimiento del menor en los casos que se preste por sí mismo, es válido únicamente para el tratamiento de los datos que le conciernen; no se puede utilizar al menor para obtener información de su núcleo familiar, excepto identidad y dirección del representante legal cuando el menor no esté capacitado para prestar el consentimiento por sí mismo.

En lo atinente al apartado tres, se incide en la necesidad de que *“La información dirigida a los menores se exprese en un lenguaje de fácil comprensión, adaptado al nivel de entendimiento que pueda tener un menor de edad, lo que obliga a utilizar un lenguaje sencillo y fácil de comprender por el menor de acuerdo con sus especiales condiciones de madurez”*, de tal manera que *“Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo”*. Este apartado indica cómo debe redactarse la cláusula informativa y además utilizarse un lenguaje sencillo que permita su comprensión por el menor evitando así un lenguaje técnico o formal; pero nada se dice sobre cómo y cuándo dar esta información,

acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos”.

¹⁰¹ BARTOLOMÉ TUTOR, ob. cit., p. 286.

por lo que habrá que aplicar los criterios generales¹⁰². Todo ello, deberá ponerse además en relación con el ya analizado citado art. 5 LOPD.

En lo que respecta al apartado cuatro exige al responsable del fichero acreditar que *“Ha obtenido el consentimiento y que éste ha sido prestado por los padres o representantes legales”*, siendo la forma escrita la más segura, planteando dudas respecto al empleo de fórmulas incluidas en una web, en las que queda constancia sobre la prestación del consentimiento aunque no sea por medio escrito. Y por eso, mantiene que *“Corresponderá al responsable del fichero o tratamiento, articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales”*. Tal previsión, ha sido ratificada por el TS en dos Sentencias de fecha 15 de julio de 2010¹⁰³.

Por último, hay que tener en cuenta que el incumplimiento del consentimiento, al igual que el deber de información, supone una infracción de la normativa de protección de datos (art. 44.3 b)¹⁰⁴, lo que puede conllevar importantes sanciones pudiendo ser rebajadas o sustituidas por un mero apercibimiento si concurren algunas de las causas que atenúan la responsabilidad previstas en los apartados 5º y 6º del art. 45 LOPD¹⁰⁵. Así, en la Resolución de 22 de diciembre de 2011¹⁰⁶ se sanciona con una multa de 20.000 euros al canal infantil Turner Broadcasting España que promocionaba la asistencia a la Cabalgata de Reyes; en la Resolución de 12 de febrero de 2015¹⁰⁷ se sanciona con una multa de 15.000 euros a un Banco por reclamar una deuda a un menor de trece años; y en la Resolución de 12 de enero de 2016¹⁰⁸ se apercibe previamente a la sanción a una Parroquia consecuencia de utilizar los datos de la menor para fines de publicidad distintos a los autorizados. Por parte de nuestra jurisprudencia, resultan particularmente interesantes la SAN de 2 de enero de 2013¹⁰⁹, en la que se condena por la difusión efectuada por un usuario de Facebook de un vídeo en su muro, libremente accesible a cualquier usuario de dicha red social, en el que éste aparece conversando con un grupo de escolares menores de edad (de entre 7 y 8 años) que miran a la cámara y cuyo rostro resulta identificable sin que dicho usuario de la red social hubiera obtenido para dicha difusión el consentimiento de sus padres o tutores; y la SAN de 26 de septiembre de 2013, relativa al acceso al Smartphone de un menor de doce años por parte del Director y del

¹⁰² Pueden consultarse, las recomendaciones para el sector del comercio electrónico realizadas por la AEPD año 2000 https://www.agpd.es/portalwebAGPD/canal/documentacion/recomendaciones/common/pdf/recomendaciones_comercio_electronico.pdf.

¹⁰³ Dictadas por la Sala de lo Contencioso-administrativo, Sección 6ª (RJ 2010, 6271 y RJ 2010, 6272). Estas sentencias resuelven ambos recursos (23 y 25/20008) interpuestos por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y por la Federación de Comercio Electrónico y Marketing (FECMD), por los que se pretendía que se declarara la nulidad de diversos preceptos del RLOPD, por infringir la LOPD y la Dirección comunitaria de protección de datos personales.

¹⁰⁴ Su vigente redacción ha sido aprobada por Ley 2/2011, de 4 de marzo, de Economía Sostenible.

¹⁰⁵ Vid. Informe Jurídico de la AEPD 0197/2013. En el que se hace un estudio pormenorizado del citado art. 13 RLOPD, emitido como consecuencia de la consulta planteada sobre si la red social deportiva está autorizada a publicar material audiovisual en que aparecen menores, cuya mecánica consiste en que los participantes suban su material a canales privados de Youtube que después se enlaza a través de la red social. La red social a que la consulta se refiere tiene a estos efectos un perfil en Facebook.

¹⁰⁶ Resolución de 3 de diciembre de 2010 sanciona por la denuncia presentada por los padres de un menor de siete años como consecuencia de una fotografía tomada a la entrada de una exposición sin su consentimiento publicada en el concurso “Fotocam” convocado por la Comunidad de Madrid, la cual fue utilizada en la composición de carteles publicitarios e incluida en una muestra itinerante y difundida en medios de comunicación. Resolución de 2 de noviembre de 2010 se sanciona a un estudio fotográfico por exponer en el escaparate del establecimiento la fotografía de un menor de edad.

¹⁰⁷ PS-00579-2014.

¹⁰⁸ A-00175-2015. Resolución de 12 de enero de 2016 de la AEPD.

¹⁰⁹ RJCA 2013,100.

Informático del Centro escolar sin el consentimiento del padre ni orden judicial, en la que se avala a un colegio que revisó el móvil de un niño por un vídeo sexual.

El art. 73 PLOPD califica de infracción grave cuando no se recaba el consentimiento del menor o del titular de su patria potestad o tutela en el tratamiento de su datos de carácter personal, o si no se acredita la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo y el art. 76 sanciona conforme a lo dispuesto en el apartado 4 del art. 83 del Reglamento (UE) 2016/679 que establece multas administrativas con un máximo de 10.000.000 euros o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, pudiendo optarse por la de mayor cuantía. Si bien hasta ahora la actuación de la AEPD ha sido prudente al sancionar, pues adecuándose a la antijuridicidad y culpabilidad de la conducta concreta imponía multas sustancialmente inferiores a las previstas en la ley por entender que concurrían circunstancias que así lo aconsejaban, a partir de la nueva LOPD habrá que ver cómo se van a cuantificar las sanciones.

De todo lo que antecede se puede concluir que la legislación da soluciones diferentes en función de qué derecho se vulnere, así en materia de protección de datos, se establece un límite expreso cual es la edad como presunción iuris tantum, por lo tanto cede la determinación de la madurez a favor de la edad como medida de seguridad jurídica; mientras que en relación al derecho al honor, intimidad e imagen se requieren condiciones de madurez. Ello nos puede llevar a preguntarnos ¿cuál es la causa de que exista un tratamiento diferente entre los derechos de la personalidad que se ejercitan en el mismo medio (Internet)? A mi parecer la explicación hay que buscarla en las fechas en que se redactaron estas leyes, pues en el caso de la LOPDH, en el año 1982 ni siquiera se podía prever los efectos que la difusión masiva de este medio podía aparejar, y en cuanto a la LOPD, en el año 1999, se elaboró en los prolegómenos del nacimiento de Internet, en la que ni tan siquiera todavía habían proliferado las redes sociales.

2.2. REGULACIÓN EN LA UNIÓN EUROPEA

2.2.1. El marco normativo vigente en materia de protección de los datos personales

Por la UE, la piedra angular de la legislación vigente en materia de protección de datos (hasta el Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril de 2016), ha sido la Directiva general 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, complementada con la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Los aspectos clave de la citada Directiva comunitaria en materia de protección de datos son: El establecimiento del principio de calidad de los datos, de tal forma que los datos personales deben ser adecuados, pertinentes y no excesivos, conforme a la finalidad para la que serán tratados; se impone como principio básico y esencial para el tratamiento de datos personales, la existencia del consentimiento previo y explícito del interesado, que ha de ser informado antes de que proceda a dicho tratamiento; se requiere a los Estados que establezcan la obligación de conciliar el derecho a la intimidad en el tratamiento de los datos personales con el derecho a la libertad de expresión; se establecen

como principios básicos de los ciudadanos los derechos ARCO en relación a sus datos personales; se incorpora como principio básico la garantía de confidencialidad, así como la obligación de implantar las medidas de seguridad oportunas que garanticen que el acceso a la información se encuentra limitado y controlado; se enuncian los principios básicos para la creación de las Autoridades Nacionales de Protección de Datos; se fijan las bases de las transferencias internacionales de datos personales; se promueve la elaboración de Códigos de conducta sectoriales, destinados a contribuir a la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales; y por último, se crea el Grupo de Trabajo del Artículo 29, institución de referencia en esta materia de Protección de Datos¹¹⁰.

Cabe decir, que con la mencionada Directiva se produjo una evolución fundamental en todos los Estados miembros de la UE, al tener la obligación de transponer a su derecho nacional una norma específica, consiguiéndose con ello un objetivo claro de armonización real, efectivo y fijándose el estándar de los motivos que pueden justificar el tratamiento legítimo de datos de carácter personal para todos los Estados miembros de la UE¹¹¹.

Con posterioridad, se han aprobado una serie de Directivas específicas como fueron la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, derogada por la Directiva 2002/58/CE del Parlamento europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y finalmente la Directiva 2009/136/CE, de 25 de noviembre del Parlamento Europeo y del Consejo de 25 de noviembre, relativa al servicio universal que modificó varias directivas del sector de las telecomunicaciones y en concreto la anterior.

Otra Directiva que también merece especial mención en esta materia, es la 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de julio de 2000, relativa a determinados particulares jurídicos sobre los servicios de la Sociedad de la Información, de la que nacen los Códigos de Conducta¹¹², siendo transpuesta a nuestro ordenamiento por la LSSI, refiriéndose expresamente a estos Códigos pero en relación a los menores de edad en su art. 18.2, expresa que *“Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad*

¹¹⁰ Se trata de un órgano consultivo independiente compuesto por: representantes de las autoridades nacionales de protección de datos de los Estados miembros, representantes del Supervisor Europeo de Protección de datos (SEPD) y un representante de la Comisión; que elabora Recomendaciones, Dictámenes y Documentos de trabajo; la Comisión desempeña funciones de secretaría del Grupo.

¹¹¹ A este respecto vid. la STJUE (Sala Tercera) de 24 de noviembre de 2011 sobre: *“Tratamiento de datos personales–Directiva 95/46/CE-art. 7, letra f)–Efecto directo”* en los asuntos acumulados C468/10 Y C469/10, que tiene por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al art. 267 TFUE, por el T S (España), mediante resoluciones de 15 de julio de 2010, recibidas en el Tribunal de Justicia el 28 de septiembre de 2010, en los procedimientos entre Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (asunto C468/10), Federación de Comercio Electrónico y Marketing Directo (FECMD) (asunto C469/10) y la Administración del Estado. En ella se declara que el art. 7, letra f), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesarios para la satisfacción del interés legítimo o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista el consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes, tal y como hace la LOPD española. Además, afirma que el art. 7, letra f), de la Directiva 95/46 tiene efecto directo.

¹¹² Considerando 49 *“Los Estados miembros y la Comisión fomentará la elaboración de Códigos de conducta; ello no irá en perjuicio del carácter voluntario de dichos códigos ni de la posibilidad de que las partes interesadas decidan libremente sin adhesión a los mismos”*.

humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias”.

Por otra parte, la Constitución Europea aprobada por unanimidad el 18 de junio de 2004 por los Jefes de Estado o de Gobierno de los veinticinco (25) estados miembros que formaban la UE en aquel momento, también recoge la protección de datos de carácter personal en sus arts. I-51¹¹³ y II-68¹¹⁴.

Pero además de todo lo anterior, se debe tener en cuenta la Carta de los Derechos Fundamentales de la Unión Europea de fecha 7 de diciembre de 2000 la cual consagra en su art. 8 como derecho fundamental la protección de datos de carácter personal, si bien no tuvo un efecto jurídico pleno y vinculante hasta el 1 de diciembre de 2009, fecha de entrada en vigor del Tratado de Lisboa o más propiamente expresado, el Tratado de Funcionamiento de la Unión Europea (TFUE) que consagra como principio en su art. 16.1¹¹⁵ que “*Toda persona tiene derecho a la protección de sus datos personales*”; además, en su apartado 2, introduce una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal.

En definitiva, la rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales, que ha llevado al Consejo de Europa a invitar a la Comisión a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas. Y así, en su resolución sobre el Programa de Estocolmo, el Parlamento Europeo acogió favorablemente un régimen general de protección de datos en la UE y, abogó entre otras cosas, por la revisión de la Decisión Marco. En su plan de acción por el que se aplica el Programa de Estocolmo, la Comisión subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplicara de forma coherente en el contexto de todas las políticas de la UE; y en su Comunicación “Un enfoque global de la protección de los datos personales en la Unión Europea”¹¹⁶, concluyó que la UE necesita una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal. De ahí, que la vigente Directiva haya sido derogada por el Reglamento general de protección de datos europeo 2016/679, aprobado en fecha 27 de abril de 2016¹¹⁷.

No obstante, mi crítica en relación al tratamiento de los datos personales de los menores de edad es la inexistencia de una normativa específica en la UE que haga referencia únicamente a la protección de este colectivo. Las Directivas 95/46/CE y

¹¹³ Art. I-51 “*Protección de datos de carácter personal: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes*”.

¹¹⁴ Art. II-68 “*Protección de datos de carácter personal: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente*”.

¹¹⁵ Art. 16.1 “*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre la protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente art. se entenderán sin perjuicio de las normas específicas previstas en el art. 39 del Tratado de la Unión Europea*”.

¹¹⁶ COM/2010/0609 final-4 de noviembre de 2010 (No publicada en el Diario Oficial). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al comité de las Regiones “Un enfoque global de la protección de los datos personales en la Unión Europea”.

¹¹⁷ El Reglamento puede consultarse en: www.boe.es/doue/2016/119/L00001-00088.pdf.

20002/58/CE no establecen ningún tipo de disposición especial dirigida a la protección de datos de los menores de edad, dejando a las regulaciones nacionales y de menor rango la adopción de medidas concretas al respecto y apostando por una autorregulación; asimismo, pese al proceso de reforma y avance que conllevan el Reglamento y Directiva del Parlamento europeo, aún no se ha podido salvar la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea¹¹⁸.

2.2.2. El Reglamento general de protección de datos de la UE 2016/679, de 27 de abril de 2016

En el nuevo y complejo entorno digital actual, tal como se analizaba en la Comunicación de la Comisión al Parlamento Europeo¹¹⁹, las normas vigentes no aportaban ni el grado de armonización requerido ni la eficacia necesaria para preservar el derecho a la protección de datos personales, motivo por el cual la citada Comisión europea propuso un marco europeo de protección de datos para el siglo XXI.

En ese sentido, según encuesta realizada en el Euro barómetro, la gran mayoría de las personas consideran que la comunicación de sus datos personales forma cada vez más parte de la vida moderna¹²⁰. Concretamente en Europa, el 72% de los usuarios de Internet siguen preocupados ante la excesiva cantidad de datos personales que se solicita en línea¹²¹ y tienen la sensación de haber perdido el control sobre sus datos personales, al no recibir información adecuada acerca de su destino, a quien se transmiten y con qué fines; sirva de ejemplo el caso de un estudiante europeo suscrito a un servicio de red social que decide solicitar acceso a todos sus datos personales archivados en la red, es entonces cuando se da cuenta de que esos datos son muchos más de los que había imaginado y de que algunos de ellos, que en teoría, habían sido suprimidos, se siguen conservando.

Por ello, la Comisión Europea con el fin de establecer un marco moderno más sólido, coherente y global en materia de protección de datos en la UE, con una aplicación estricta que permitiera el desarrollo de la economía digital en el mercado interior, que otorgase a los ciudadanos el control de sus propios actos y reforzase la seguridad jurídica y práctica de los propios operadores económicos y las autoridades públicas, propuso una sola normativa para toda la UE que resistiera el paso del tiempo; así, independientemente de cómo evolucionasen en el futuro la tecnología y el medio digital, la información personal de los ciudadanos de la UE estaría siempre segura y se respetaría su derecho fundamental a la protección de sus datos.

El nuevo marco jurídico europeo para la protección de datos personal, se ha configurado a través de la aprobación en fecha 25 de enero de 2012 de una Propuesta de Directiva del Parlamento Europeo y del Consejo (DEPD), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y de una Propuesta de Reglamento del Parlamento y del

¹¹⁸ Euro barómetro especial (EB), Data Protection and Electronic Identity in the EU (Protección de datos e identidad electrónica en la UE, 2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

¹¹⁹ Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones. La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI.COM (2012) 09 final. Disponible en <http://eur-lex.europa.eu/legal/52012DC0009>.

¹²⁰ Euro barómetro especial nº 359, Actitudes hacia la protección de datos y la identidad electrónica en la Unión Europea, junio de 2011, p. 23.

¹²¹ Ibídem, apartado 54.

Consejo (RGPD), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos; siendo publicados en fecha 27 de abril de 2016 en el DOUE ya como Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, y como Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, y aunque su entrada en vigor será a los veinte días de su publicación (es decir, a partir del 25 de mayo de 2016) únicamente el Reglamento es aplicable a partir del 25 de mayo de 2018.

En cuanto al ámbito de aplicación del nuevo RGPD¹²², la Comisión Europea ha elegido como instrumento jurídico más apropiado para la nueva regulación de la protección de datos personales el reglamento y ello, por entender que ofrece mayor seguridad jurídica; por consiguiente, el Reglamento europeo, “será obligatorio en todos sus elementos y directamente aplicable en cada estado miembro” sin necesidad de transposición alguna, de manera que su aprobación desplazará a la legislación nacional y autonómica, tal como indica TRONCOSO REIGADA¹²³, lo que conlleva derogar la normativa reglamentaria de desarrollo de la LOPD que resulte incompatible con las cuestiones reguladas en el citado Reglamento y la Directiva 95/46/CE. Si bien, deberán seguir en vigor las decisiones de la Comisión adoptadas y las autorizaciones dictadas por las autoridades de control sobre la base de la Directiva 95/46/CE. Respecto de las materias no reguladas en el Reglamento, se regirán por la legislación nacional siempre que no sean contrarias a los principios establecidos en aquél¹²⁴. Asimismo, la legislación nacional presidirá cuando se traten datos en el ejercicio de actividades no comprendidas dentro del ámbito de aplicación del Derecho de la UE, por ejemplo política exterior o seguridad nacional¹²⁵. Cabe recordar, que al igual que ya se ha regulado a nivel nacional, no debe aplicarse al tratamiento por una persona física de datos de carácter personal que sean exclusivamente personales o domésticos, como la correspondencia y la llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por tanto, sin conexión alguna con una actividad profesional o comercial. La exención tampoco se aplicará a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.

En relación a los menores, el Reglamento tampoco se refiere únicamente al tratamiento de datos personales de los menores de edad; tan sólo introduce un precepto específico en esta materia consecuencia de la regulación de otras cuestiones a lo largo de su articulado, pero partiendo siempre de ese principio de especial protección. En general, recoge criterios básicos sobre la protección de datos personales de menores que se venían apuntando en los últimos años y en particular, se centra en el consentimiento de este colectivo en relación con el tratamiento de sus datos personales en los servicios de la sociedad de la información.

2.2.3. El consentimiento del menor en el tratamiento de sus datos personales

¹²² Vid. Considerando 10 del Reglamento. No obstante, es una cuestión controvertida la utilización de este instrumento jurídico.

¹²³ TRONCOSO REIGADA, A., “Hacia un nuevo marco jurídico europeo de la protección de datos personales”, *Revista Española de Derecho Europeo*, nº 43, julio-septiembre 2012, pp. 25-184.

¹²⁴ El Dictamen del Consejo Económico y Social Europeo sobre la propuesta de Reglamento de 23 de mayo de 2012 (DOUE 31/7/2012) considera que se debería permitir a los Estados miembros adoptar, en su legislación nacional, disposiciones no incluidas en el Reglamento o más favorables que las previstas en el mismo, tal y como se recoge en los arts. 80 a 85 del Reglamento.

¹²⁵ El art. 2.4 del Reglamento dice, por otra parte, que deja a salvo la aplicación de la Directiva 2000/31/CE, sobre comercio electrónico, en particular, en lo relativo a la responsabilidad de los prestadores de servicios de intermediación de conformidad con los arts. 12 a 15 de dicha Directiva.

El RGPD, define en su art. 4.11 con carácter general, en qué consiste el “consentimiento del interesado”, pero la problemática y crítica que surge en torno a dicho consentimiento es la redacción del citado precepto que permite concluir que sea siempre expreso y no tácito¹²⁶. Con respecto a su validez y licitud se regula en sus arts. 6 y 7; de tal modo, que la carga de demostrar que el tratamiento se ha llevado a cabo con el consentimiento del interesado corresponde al responsable del tratamiento, en particular, en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente de dar su consentimiento y en qué medida lo hace¹²⁷.

Ahora bien, cuando se trata de un menor de edad, la novedad en la Propuesta del Reglamento correspondía en primer lugar, a la definición de “niño” como toda persona menor de 18 años conforme con lo establecido en la Convención de la Organización de las Naciones Unidas (ONU), sobre los derechos del niño, de 20 de noviembre de 1989¹²⁸; pese a ello, el nuevo Reglamento en su considerando 38¹²⁹ ha eliminado tal referencia. Y en segundo lugar, al art. 8, que se dedica específicamente al tratamiento de los datos personales de los niños en relación con la oferta directa de servicios de la sociedad de la información; de tal manera, que su apartado 1º, establece que el tratamiento de los datos personales relativos a los niños menores de 16 años solo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño¹³⁰. En la propuesta de Reglamento

¹²⁶ De esta forma el consentimiento sería únicamente expreso y en cambio, a diferencia de la regulación contenida en los arts. 7.3 y 2 de la LOPD, no se contempla los supuestos de consentimiento expreso (origen racial, salud y vida sexual), y consentimiento expreso y por escrito (ideología, afiliación sindical y creencias). MARTÍNEZ MARTÍNEZ, R., Jornada sobre el Reglamento de Protección de Datos organizado por la extinta Agencia de Protección de Datos de la Comunidad de Madrid: “Se apuesta por el Opt-in; no cabría el consentimiento tácito”. Resúmenes de este evento: “Conclusiones sobre la jornada del Reglamento de Protección de Datos de la UE organizado por la APDCM” de F. J. SEMPERE SAMANIEGO: [http:// Fja/2012/05/23/conclusiones-jornada-reglamento-pdatos-de-la-ue-de-la-apdcm/](http://Fja/2012/05/23/conclusiones-jornada-reglamento-pdatos-de-la-ue-de-la-apdcm/) “Jornada sobre el proyecto de Reglamento de la APDCM” de L. SALVADOR MONTERO: <http://www.privacidadlogica.es/2012/05/22/jornada-sobre-el-proyecto-de-reglamento-por-la-apdcm/>. Tradicionalmente se usaba el sistema OPT-OUT, es decir, que la casilla venía directamente marcada (en la práctica se suele utilizar también para determinadas páginas web) cuando lo más lógico es un sistema OPT-IN en el que el particular pueda otorgar su consentimiento libremente.

¹²⁷ Art. 7. “1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato”.

¹²⁸ Considerando 29 “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos en relación con el tratamiento de datos personales. Con el fin de determinar cuándo se considera que una persona es un niño, el presente Reglamento debe asumir la definición establecida en la Convención de las Naciones Unidas sobre los derechos del niño”.

¹²⁹ Considerando 38. “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños”.

¹³⁰ Art. 8. “1 Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta

se refería a los menores de 13 años¹³¹ y daba a entender que, a efectos del consentimiento de los menores, se diferenciaba el mundo on line del real porque establecía el límite de los 13 años solo cuando se trataba de “oferta directa de servicios de la sociedad de la información”, con lo que se podía llegar a la absurda conclusión de estar ante un consentimiento de los menores hasta 18 años ligado a lo que dispone el CC en el mundo físico, y en cambio, en Internet se consentiría a partir de los 13 años. Para evitar tal confusión, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE), había eliminado el término “de la sociedad de la información”. Por consiguiente, la edad de 13 años era aplicable cuando se trataba de “oferta de bienes y servicios dirigidos a los menores”, cuestión bastante lógica ya que suponía igualar los dos “mundos” como acertadamente ha señalado JAVIER SEMPERE¹³². Pese a lo manifestado, el actual art. 8.1 RGPD introduce nuevamente en su redacción “*oferta directa a niños de servicios de la sociedad de la información*”. Por otra parte, SEMPERE SAMANIEGO¹³³ ha criticado las diferentes edades que se recogían en la Propuesta pues argumentaba que no entendía muy bien esa diferenciación de los 13 años para el consentimiento y por otra parte que la definición de menor abarcase hasta los 18 años, llegando a pensar si ello significaba que sería necesario 13 años para consentir y 18 para el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), por tanto, abogaba por recoger solo la edad de los 13 o 14 años para el consentimiento y el resto de actos relativos a la protección de datos personales. Hay que decir, que con la aprobación del RGPD, desaparece la definición de menor y se establece únicamente una edad. Además, tal como manifiesta PIÑAR MAÑAS¹³⁴, a partir de ahora, “Se acabaron en España los conocidos derechos ARCO”, pues la normativa se referirá a los derechos de transparencia, información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos y oposición.

En cuanto a las razones que llevaban a establecer el límite en los 13 años eran porque tenía en cuenta la normativa americana y no la española (14 años). En relación a la fijación de un límite de edad, han existido opiniones doctrinales totalmente opuestas. Mientras SEMPERE SAMANIEGO¹³⁵ considera que establecer una edad del tratamiento de datos de menores, sea cual fuere, suponía dar seguridad jurídica a los responsables y encargados, en cambio, PEDRO GRIMALT, con ocasión del SIRCAM celebrado en

la tecnología disponible. 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño”.

¹³¹ Art. 8. Propuesta del Reglamento. “1. A efectos del presente Reglamento, en relación con la oferta directa de servicios de la sociedad de la información a los niños, el tratamiento de los datos personales relativos a los niños menores de 13 años solo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño. El responsable del tratamiento hará esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible. 2. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como son las normas en materia de validez, formación o efectos de los contratos en relación con un niño. 3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el art. 86, a fin de especificar los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable contemplados en el apartado 1. Para ello, la Comisión se planteará la adopción de medidas específicas para las microempresas, las pequeñas y medianas empresas. 4. La Comisión podrá establecer formularios normalizados para los métodos específicos de obtención del consentimiento verificable contemplados en el apartado 1. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el art. 87, apartado 2”.

¹³² JAVIER SEMPERE, F., Artículo de fecha 9 de diciembre de 2013, “Reglamento Protección de datos de la UE: el consentimiento de los menores”, publicado en <http://privaciadlogica.es>.

¹³³ SEMPERE SAMANIEGO, ob. cit., p. 129.

¹³⁴ En Jornadas Enatic sobre el Nuevo Reglamento Europeo de protección de datos disponible en <http://noticias.juridicas.com/actualidad/noticias/11047-el-nuevo-reglamento-europeo-de-proteccion-de-datos:un-texto-complejo-que-abre-nuevas-perspectivas-profesionales-a-la-abogacia>.

¹³⁵ SEMPERE SAMANIEGO, ob. cit., p. 92.

Murcia¹³⁶, entiende que debería acudirse a las normas del derecho civil que se decantan por la madurez del menor en vez de establecer una edad. En similar dirección, otros Reglamentos de Protección de Datos, como el de Perú¹³⁷ o México¹³⁸ han fijado la edad del consentimiento en 14 años, probablemente influidos por la normativa española. En cualquier caso, ni el Grupo del Art. 29 ni el Supervisor Europeo de Protección de Datos, han analizado en sus Informes si la edad debe ser “13” o “14” u otra. Quien sí ha elaborado un Informe¹³⁹ es la European Consumer Association, por estimar que podían existir problemas a la hora de cumplir con la obligación del consentimiento parental, ya que la edad de 13 años podía ser contraria a las normas generales de cada país que regulaban la capacidad de los menores de edad para contratar, y había incidido en que una cosa era el tratamiento de datos de un menor de 13 a 18 años para participar, por ejemplo, en un concurso y otra contratar. El problema surgía cuando de ese tratamiento se podía derivar la firma de un contrato, como puede ser la instalación de un Apps en su teléfono móvil, ya que la aceptación de las diferentes cláusulas de la respectiva Apps deriva en la firma aunque virtual de un contrato. Añadía que habría que diferenciar la legitimación parental¹⁴⁰ del posible control de tratamiento de datos, pues podría ser excesivo, y en último lugar, mantenía que no se debía dejar a la Comisión el desarrollo de este precepto, ya que dada su importancia debería recogerse en la citada Propuesta las formas para recabar el consentimiento parental. Según apunta LÓPEZ CALVO¹⁴¹, con el nuevo RGPD en muchos casos la prestación del consentimiento se va a asemejar mucho a un contrato de adhesión sin margen de negociación para los particulares.

En lo que respecta a los mecanismos de verificación de edad establecidos para comprobar la edad, en la práctica se ha demostrado que ninguno de ellos es fiable, salvo el DNI electrónico que en España ya es posible, en virtud del RD 869/2013 que modifica el RD 1553/2005 de 23 de diciembre por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica. Concretamente, en su art. 1.4 párr. segundo, se prevé que el documento de identidad de los menores contendrá una identificación electrónica, para la que se activará un certificado de autenticidad. Con ello, los proveedores de servicios en Internet tienen una herramienta -no la única- que les permite cumplir con la obligación de verificar la edad de los menores. De acuerdo con esto, el Informe de la Comisión Europea sobre soluciones de verificación de edad elaborado a propósito del Fórum sobre un Internet más seguro, expone diferentes métodos

¹³⁶ SIRCAM es un foro Anual sobre la Sociedad de la Información organizado por la Región de Murcia, y de la que es impulsor su Universidad.

¹³⁷ Reglamento de la Ley de Protección de Datos Personales del Perú 3/2013, Art.27 “*Para el tratamiento de los datos personales de un menor se requerirá el consentimiento de los titulares de la patria potestad o tutores según corresponda*”. Art. 28 “*Podrá hacerse tratamientos de datos personales de los mayores de 14 años y menores de 18 años con su consentimiento, siempre que la información proporcionada haya sido expresada en un lenguaje comprensible por ellos, salvo en los casos que la ley exija para su otorgamiento la presencia de los titulares de la patria potestad o tutela. En ningún caso, el consentimiento para el tratamiento de los datos personales de los menores de edad podrá otorgarse para que accedan a actividades, vinculadas con bienes o servicios que están restringidos para los mayores de edad*”.

¹³⁸ Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 21 de diciembre de 2011. Art. 89 in fine “*Para el ejercicio de los derechos ARCO de datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se estará a las reglas de representación dispuestas en el Código Civil Federal*”.

¹³⁹ Dictamen de la European Consumer Association. Position Paper, p. 16, <http://www.beuc.org/BEUCNoFrame/Docs/2/EMCCOKNDDMCAHGPOAJPLPKIGPDWY9D1AY9DW3571KM/BEUC/docs/DLS/2012-00531-01-E.pdf>

¹⁴⁰ Sobre el papel de los padres y más concretamente, referido al control parental- monitorización por parte de los padres del uso del ordenador que hacen los menores- interesante la postura defendida por Noemí Brizo Izquierdo en el II Congreso Nacional de Privacidad organizado por la Asociación Profesional Española de Privacidad, celebrado el 13 y 14 de junio de 2013 en Madrid, que puso en duda incluso la legalidad del mismo ya que puede afectar al libre desarrollo de la personalidad del menor.

¹⁴¹ En Jornadas Enatic sobre el Nuevo Reglamento Europeo, ob. cit., p. 2.

de verificación on line¹⁴² como pueden ser por ejemplo, la auto-certificación o auto-declaración (el usuario es el que dice que tiene la edad correspondiente); el uso de tarjetas de crédito o débito (se pueden utilizar para esta finalidad si bien en el caso de menores es dudoso que las posean); las tarjetas de identidad electrónica (eID), que son las tarjetas con chip, que incorporan certificados electrónicos o firma digital, como el DNI electrónico, que es obligatorio a partir de los 14 años; en este caso, su rápida implementación y su fiabilidad es una ventaja, pero el inconveniente es el exceso de información y la necesidad de lectores adicionales (no todos los menores lo tienen y en su caso incorpora funcionalidades limitadas); el análisis semántico (es un método que determina la edad mediante frases y palabras más comúnmente utilizados por los menores); los números de Seguridad Social e identificadores nacionales (cabe recordar que en España no es obligatorio el DNI para los menores de 14 años); la biometría (el uso de la tecnología que por medio de la captura de huellas digitales, medición de la densidad de los huesos, las exploraciones de iris y otras diferencias biológicas, es capaz de determinar la edad de los usuarios, al menos dentro de un cierto rango) y la verificación off line, el control físico y control de los padres (este sistema conlleva que el usuario se presente físicamente para la comprobación de edad y contrastar con documentación o identificadores como el DNI, es un método comúnmente utilizado por los operadores móviles en el punto de venta para dispositivos móviles).

Prosiguiendo con el análisis del citado art. 8 de la Propuesta del Reglamento, en concreto sus apartados 3 y 4, la Comisión se reservaba la facultad de adoptar actos delegados, para especificar los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable. Al efecto, se plantearía la adopción de medidas específicas para las microempresas, las pequeñas y medianas empresas, así como establecer formularios normalizados para los métodos específicos de obtención del consentimiento verificable. En la actualidad, no hay ningún sistema que pueda garantizar esa verificación en la recogida de datos vía on line, por lo que el responsable se encuentra en situación de indefensión. Quizás la forma más segura sea poder descargar un formulario de la página web a través del cual se pueda prestar y facilitar su consentimiento mediante envío con una copia DNI de los padres o tutores por correo electrónico. Finalmente, cabe decir que tales apartados han sido eliminados del art. 8 del RGPD.

Por otra parte, el nuevo Reglamento, en lo concerniente a la forma de obtener el consentimiento se condiciona teniendo en cuenta el estado de la tecnología, es decir, se introduce el principio de calidad de los datos personales para no recabar aquellos que no sean necesarios para la finalidad para la cual se recogen. También se añade que la información facilitada a los niños, padres o tutores a la hora de obtener el consentimiento y recabar los datos personales, sea sencilla y comprensible, especificación que, a su vez, ya había recogido la Propuesta del Reglamento en su considerando 46 (39 y 58 en el RGPD). El catálogo de los mecanismos citados, corresponde al “European Data Protection Board” (denominado Consejo Europeo de Protección de Datos o CEPD), pero limitando su actividad, ya que únicamente ofrecerán recomendaciones, buenas prácticas o guías al efecto es decir, se pasa de una especie de regulación de estos mecanismos, vía Comisión, a una labor consultiva a realizar por el CEPD, pero sin perder de vista la aplicación del principio de confianza legítima.

Por todo lo expuesto, cabe concluir que, si bien la Propuesta del Reglamento se decantaba por buscar una edad fijada en 13 años para todos los países de la UE, con el fin de dar uniformidad y seguridad jurídica a los responsables y encargados de las distintas redes sociales, el nuevo Reglamento eleva el límite a los 16 años y da libertad a los

¹⁴²“Verificación de la edad en Internet” de S. BERNELL en <http://ticyprivacidad.es/2011/02/10/verificacion-de-edad-en-internet/>.

Estados miembros para establecer por ley otra edad siempre que esta no sea inferior a 13 años. Consecuentemente, nuestra actual normativa (art. 13 del RDLOD o el art. 1.4 del RD 869/2013) podrá ser aplicable sin más, toda vez que su límite está en los 14 años, o decantarse por rebajar la edad a los 13 años en adelante o elevar el límite hasta los 16 años, con la correspondiente reforma de las citadas normas, en este sentido, ha optado por una nueva LOPD en la que se establece los 13 años en adelante como edad mínima para consentir. Con ello, evita ahondar aún más si cabe en la ya actualmente existente cuestión espinosa cual es la de ceder la determinación de la madurez en favor de la edad como medida de seguridad jurídica. Ahora bien, a la vista de las expectativas generadas por la citada norma, considero que ha sido poco ambiciosa en relación a los menores de edad, pues debería haber extendido su ámbito de aplicación a otras cuestiones más allá del citado art. 8; definiendo los mecanismos de control que podrían aplicar los encargados y responsables del tratamiento para asegurar una navegación segura de los menores e incidiendo aún más en el principio del deber de información de los responsables del tratamiento, de tal manera que el menor de edad reciba una información suficiente en el tratamiento de sus datos, y no insuficiente, como en la práctica está ocurriendo en los diferentes países de la UE, de forma discordante e incorrecta en muchas ocasiones por parte de los responsables y encargados del tratamiento.

2.2.4. Otras medidas dirigidas a la protección del menor. El derecho al olvido

En relación al menor de edad, una de las medidas incluidas en el citado Reglamento es “la licitud en el tratamiento de los datos”. Así en su art. 6 establece uno de los supuestos en los que es lícito el tratamiento *“Cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de los datos personales, en particular, cuando el interesado sea un niño”* y lo desarrolla en el considerando 47¹⁴³. En estos casos, normalmente prevalece la protección del menor, debiendo en consecuencia ampararse el tratamiento de sus datos para que sea lícito en alguno de los otros casos previstos en el citado art. 6.

Otra medida es la “transparencia”, de manera que la información y comunicación que el responsable del tratamiento de datos personales facilite al usuario debe ser transparente, utilizar un lenguaje sencillo, claro y adaptado al interesado y en particular para cualquier información dirigida específicamente a los niños (art. 12.1¹⁴⁴ y

¹⁴³ Considerando 47. *“El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo”*.

¹⁴⁴ Art. 12.1 *“El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo,*

considerando 58¹⁴⁵). De modo que, en el caso de la información dirigida a los menores debe facilitarse en un lenguaje adaptado a sus posibilidades de comprensión como ya se recogía en la Exposición de Motivos de la Propuesta del Reglamento¹⁴⁶, dimanante a su vez de la Resolución de Madrid 2009 sobre la adopción de estándares internacionales¹⁴⁷. Finalmente, el Grupo de Trabajo del Art. 29 en fecha 13 de marzo de 2013, ha aprobado el primer Dictamen conjunto sobre la privacidad en las aplicaciones móviles¹⁴⁸.

Por otra parte, otras medidas a destacar son “las basadas en la elaboración de perfiles” (art. 22), y si bien no se hace referencia expresa a los menores; sin embargo, en el considerando 71 se señala que para los supuestos excepcionales en que pueden admitirse estas medidas, en ningún caso deberán afectar a un menor. Asimismo, los llamados “Códigos de conducta” (art. 40. 2. g) los cuales (entre los diferentes sectores de tratamiento de datos) deberán tener en cuenta las características específicas y relativas a la información y protección de los niños. También las “Campañas de sensibilización por las autoridades de control” (art. 57.1 b), que ya se venían aplicando en nuestro país con el fin de obtener mayor sensibilización de los ciudadanos y en concreto las dirigidas específicamente a los menores de edad.

Finalmente, la medida que más impacto ha causado en las redes sociales es “el derecho de supresión” (el derecho al olvido), que en el Reglamento pasa a denominarse únicamente “el derecho a la supresión de datos” conforme al cual el responsable debe abstenerse a darles más difusión, especialmente en el caso de los datos proporcionados cuando el interesado sea un niño (art. 17)¹⁴⁹. El considerando 63 hace referencia a datos

en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios”.

¹⁴⁵ Considerando 58 “El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender”.

¹⁴⁶ Propuesta de Reglamento de Protección de Datos, “El art. 11 introduce una obligación para los responsables del tratamiento de ofrecer información transparente y de fácil acceso y compromiso, inspirada especialmente en la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad”, p. 9.

¹⁴⁷ Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. http://www.agpd.es/portalwebAGPD/canal/documentacion/conferencias/common/pdfs/31conferencia_internacional/estandares_resolucion_Madrid_es.pdf.

¹⁴⁸ El Dictamen destaca que no todas las aplicaciones informan adecuadamente sobre el tipo de datos que la aplicación puede procesar y con qué fines. En este sentido, un reciente estudio refleja que sólo el 61% de las 150 aplicaciones más descargadas cuenta con una política de privacidad. En lo atinente al consentimiento, que constituye la base jurídica para permitir que una empresa trate los datos personales del usuario, las autoridades subrayan que a menudo este se reduce a una casilla de verificación que indica que el usuario acepta los términos y condiciones aplicables, sin ofrecer una opción que permita rechazarlas. Según un estudio realizado por GSMA, al 92% de los usuarios de *apps* les gustaría que se les ofreciese la opción de elegir a qué funciones de su terminal puede acceder la aplicación y a cuáles no. Los usuarios deben poder controlar sus propios datos personales. Por ello, los desarrolladores de aplicaciones deben proporcionar información suficiente sobre los datos que van a tratar antes de hacerlo, de forma que puedan obtener un consentimiento válido. El documento puntualiza que el usuario no debe enfrentarse a una pantalla cuya única opción es la de “Sí, acepto”. También debería mostrarse un botón que permitiera cancelar la instalación. Además, el usuario tiene que poder conocer a qué información va a acceder el desarrollador de la *app* antes de instalarla. En este sentido, los fines del tratamiento de esos datos tienen que estar bien definidos y deben ser comprensibles para un usuario medio, excluyéndose los cambios repentinos en las condiciones del servicio. El Dictamen destaca que el hecho de hacer clic en el botón “Instalar” no implica necesariamente un consentimiento válido para el tratamiento de datos personales si no va acompañado de suficiente información, tanto sobre las condiciones de ese tratamiento como sobre el hecho de que al pulsar “Instalar” se presta el consentimiento para tratar los datos en esas condiciones.

¹⁴⁹ Art. 17. 1. “El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en

que se otorgaron cuando el titular no era plenamente consciente de los riesgos que implicaba el tratamiento. Tal precepto ha sido criticado por ARTEMI RALLO¹⁵⁰ quien apuntaba que el art. 8 de la Propuesta del Reglamento ya otorgaba un método específico al tratamiento de los datos de los niños menores de 13 años, con lo que, desde el punto de vista estrictamente jurídico, obligaría a diferenciar el régimen de cancelación de datos en función de que éstos hubieran sido facilitados siendo niños o adultos, con lo cual o bien se estaría minorando la protección debida a los adultos, o bien se estaría duplicando las garantías ya previstas para los menores¹⁵¹. Por su parte, JAVIER SEMPERE¹⁵² reflexionaba sobre la situación paradójica que podría darse cuando el menor facilitó datos sin conocer los riesgos y posteriormente, una vez adulto quiere eliminarlos, sobre todo cuando están publicados en Internet, en cuyo caso la empresa responsable tendría que reenviar la solicitud de borrado a otras que hayan utilizado esa información. Sin embargo, para ANDREU MARTÍNEZ¹⁵³, con esta medida se ha protegido aún más las actuaciones realizadas por el menor antes de alcanzar la mayoría de edad y se evita con ello la generación de perfiles desde edad temprana.

Con relación a este derecho y aunque no se refiere a los menores de edad, es relevante la Sentencia del TJUE de fecha 13 de mayo de 2014¹⁵⁴, en la cual surge el derecho al olvido no regulado expresamente en la Directiva vigente, de manera que cualquier persona tendrá derecho a solicitar del motor de búsqueda directamente la eliminación de los datos personales que pueden afectarles, aunque la información no haya sido eliminada por parte del editor de los contenidos, ni se haya solicitado su desindexación. Con lo que se podrá solicitar a Google directamente el borrado de datos personales que aparecen en el buscador indexados y Google tendrá la obligación de borrarlos, pues si no lo hace, se podrá acudir de forma efectiva a solicitar la tutela de la AEPD o de los Tribunales en caso de conflicto. Por consiguiente, se articula la posibilidad de eliminar información personal frente al motor de búsqueda, que es el responsable de la difusión y accesibilidad de la información publicada por los diferentes portales. Si bien, la referida sentencia concreta que el derecho a la protección de datos prevalecerá con carácter general sobre el interés económico del buscador o cualquier tercero, salvo que la información sea de interés o relevancia pública que permita justificar su difusión. Por lo tanto, se deberá ponderar en cada caso la primacía del derecho a la Protección de Datos o del Derecho a la Información, que legitima en algunos casos la publicación de todo tipo

relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1”.

¹⁵⁰ ARTEMI RALLO, L., *El derecho al olvido en Internet. Google versus España*, Centro de Estudios políticos y constitucionales, Madrid, 2014, p. 46.

¹⁵¹ En este mismo sentido, se pronuncia para justificar la enmienda de supresión de esta referencia a los niños en el art. 17.1 GDPR, el Proyecto de Informe, de 16 de enero de 2013, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos elaborado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo por el Ponente Jan Philipp Albrecht.

¹⁵² JAVIER SEMPERE, ob. cit., p. 1.

¹⁵³ ANDREU MARTÍNEZ, ob. cit., p. 58.

¹⁵⁴ Planteada por la AN en relación a la interpretación y aplicación de la Directiva 95/46/CE (sobre protección de datos personales) en el caso de Mario Costeja contra Google donde finalmente se aclara la larga disputa entre la responsabilidad de los buscadores, la aplicabilidad de la normativa de protección de datos y los derechos de los ciudadanos. Concretamente se analiza sobre la libertad a decidir lo que otros pueden hacer con tu información personal.

de información. Para JAVIER SEMPERE¹⁵⁵, el futuro dirá si Google y el resto de buscadores en la misma situación cumplen con lo dictado en esta Sentencia, pues no le gustaría que ahora se dirigiese el ejercicio del derecho de oposición hacia los buscadores. En España, respecto al derecho al olvido digital cabe citar las recientes sentencias del TS de fechas 15 de octubre de 2015¹⁵⁶ y 5 de abril de 2016¹⁵⁷ que siguen la doctrina sentada por la anterior sentencia del TJUE.

En consonancia con lo anterior, debo destacar que si bien en California¹⁵⁸ se ha aprobado una ley en virtud de la cual los menores tienen derecho al olvido parcial en Internet¹⁵⁹, en la UE no existe normativa específica alguna respecto al derecho al olvido de los menores en Internet, aunque actualmente se está trabajando en un cuidadoso proyecto para que el derecho al olvido sea aplicado también a casos de menores que se vean afectados por la publicación de determinada información en la red¹⁶⁰.

3. BIBLIOGRAFÍA

ABA CATOIRA, A., “Los menores ante Internet: las redes sociales”, *www.js-e.cat/site/arxiu/pdfs/Ana-_M-Aba-Catoira-PONENCIAS.pdf*.

ANDREU MARTÍNEZ, M.B., “Diez años de aplicación de la Children’s online Privacy Protection Act estadounidense. Reflexiones para el Derecho español”, *Revista Española de Protección de Datos*, nº especial julio 2009-junio 2010, Agencia de Protección de Datos de la Comunidad de Madrid, Thomson Civitas, 2010, Madrid, p.84.

- *La protección de los datos personales de los menores de edad*, Thomson-Reuters Aranzadi, Navarra, 2013.

ARTEMIRALLO, L., *El derecho al olvido en Internet. Google versus España*, Centro de Estudios políticos y constitucionales, Madrid, 2014.

BARTOLOMÉ TUTOR, A., *Los derechos de la personalidad del menor de edad. Su ejercicio en el ámbito sanitario y en las nuevas tecnologías de la información y comunicación*, Thomson-Reuters Aranzadi, Navarra, 2015.

¹⁵⁵ JAVIER SEMPERE, F., Artículo de fecha 13 de mayo de 2014, “Reflexiones sobre la responsabilidad de Google ene. Derecho al olvido”, en <http://privacidadlógica>. Considera que el llamado “Derecho al olvido” sigue sin permitir una solución general, de manera que habrá que ir caso por caso, porque cada uno de ellos “es un mundo” pero teniendo en cuenta además la conducta del propio usuario o internauta; pues no se puede pretender que si en el año 2014 publicó un tuit que luego fue difundido en múltiples sitios, en el año 2018 quiera eliminarlo de todos, o que no lo enganchen los buscadores. Igual que debe existir una responsabilidad del que publica datos personales en una página web, debe existir también una responsabilidad por parte del usuario.

¹⁵⁶ ROJ 4132/2015.

¹⁵⁷ Id Cendoj: 28079119912016100005.Recurso 3269/2014, Ponente: Rafael Saraza Jimena.

¹⁵⁸ En fecha 24 de septiembre de 2013 se publicó en <http://www.genbeta.com/actualidad/en-california-los-menores-tendrán-derecho-al-olvido-parcial-en-internet>. “Según la nueva normativa, que entrará en vigor en 2015, los menores sí que podrán pedir que las compañías de Internet eliminen toda su actividad publicada on line. ¿Por qué? De acuerdo a lo que dicen los propios impulsores de la ley, “los errores de los adolescentes pueden permanecer toda la vida y su vida digital puede seguirlos allá donde vayan”. Para empezar, esta ley sólo es válida para menores. Los adultos seguirán sin tener derecho al olvido. Además, según la legislación las compañías deberán evitar que la información relacionada con los menores que lo soliciten sea pública pero no les obliga a eliminarla de sus servidores. Los menores que se acojan a esta nueva ley podrán pedir que se eliminen contenidos sobre ellos mismos, pero sólo los que ellos hayan publicado. Si alguien decide, por ejemplo, coger una foto comprometida de un usuario y resubirla, éste no podrá reclamar sobre la que no haya compartido él mismo.

¹⁵⁹ Consultar en <http://bibliotecaescolardigital.es/comunidad/BibliotecaEScolarDigital/recurso/en-california-los-menores-tendrán-derecho-al-olvido/fde7c94c-ac4a-4685-ad85-367a>.

¹⁶⁰ Tal como anticipó en mayo de 2014 la presidenta del Consejo de los Derechos de Niñas, Niños y Adolescentes, *Guadalupe Tagliaferri* se trata, de una novedosa iniciativa que busca poner en primer plano el derecho de los menores, que también se pueden ver afectados por la publicación de fotos, textos agraviantes o demás cuestiones que puedan colgarse de la Red y que afecte a un menor. “Es importante construir en este nuevo esquema de las tecnologías, nuevos paradigmas de relación y todo lo relacionado con la seguridad en estas plataformas. Hay que concienciar a los chicos y a los padres sobre la necesidad de no exponerse y de no maltratar al otro”. SANTIPINTOSABRINA, ssantopinto@diariobae.com. <http://www.diariobae.com/note/17913-derecho-al-olvido-para-los-menores.html>.

BUTTARELLI, G., “Los menores y las nuevas tecnologías”, en *Redes sociales y privacidad del menor*, Reus, (Dir. J. L. PIÑAR MAÑAS), Madrid, 2011.

CASTELLÓ MARTÍNEZ, A., “Ética en publicidad Online”, Fonseca, *Journal of Communication*, nº 1, ISSN: 2172-9077, p. 232.

GIL ANTÓN, A. M., *El derecho a la propia imagen del menor en Internet*, Dykinson, Madrid, 2013.

GÓMEZ HIDALGO, J. M., “Menores y Móviles, Usos, riesgos y controles parentales”, 19 de abril 2013, www.mavir.net/docs/jmgomez-uem-abr2013.pdf, p. 57.

GÓMEZ-JUÁREZ SIDERA, I., “Reflexiones sobre el derecho a la protección de datos de menores de edad y la necesidad de su regulación específica en la legislación española”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 11, 2006, p. 86.

- “La protección de los datos del menor como e-consumidor” en *Consumidores y usuarios ante las nuevas tecnologías* (Coord. I. COTINO HUESO), Tirant lo Blanch, Valencia, 2008.

GRIMALT SERVERA, P., “Los menores en internet: capacidad versus protección de la vida privada” en *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, (Coords. M. CUENA CASAS, L. A. ANGUITA VILLANUEVA y J. ORTEGA DOMÉNECH), Dykinson, Madrid, 2013.

JAVIER SEMPERE, F., “Reflexiones sobre la responsabilidad de Google ene. Derecho al olvido”, Artículo de fecha 9 de diciembre de 2012, <http://privacidadlógica.es>.

-“Reglamento Protección de datos de la UE: el consentimiento de los menores”, Artículo de fecha 13 de mayo de 2014, <http://privaciadlogica.es>.

LÓPEZ SÁNCHEZ C., *La responsabilidad civil del menor*, Dykinson, Madrid, 2001.

LUQUIN BERGARECHE, R., *La protección Jurídico-Civil del Menor Usuario de Telefonía Móvil en la Sociedad de la Tecnología*. Cuadernos de Aranzadi civil, Navarra, 2012.

MARTÍNEZ OTERO, J. M., “La protección de los menores en los medios audiovisuales en Estados Unidos”, *Derecho Comparado de la Información*, nº17, 2011, pp. 121-163.

MESSÍA DE LA CERDA BALLESTEROS J. A., “Algunas consideración sobre protección de datos personales de las personas menores de edad en Internet”, en *Los derechos de la personalidad de los menores y las nuevas Tecnologías*, (Coords. E. JORDÁ CAPITÁN y V. DE PRIEGO FERNÁNDEZ), El Derecho, Madrid, 2012.

OROZCO PARDO, G., “Intimidad, privacidad, “extimidad” y protección de datos del menor. ¿Un cambio de paradigma? “en *La Protección Jurídica de la intimidad*, (Dir. J. BOIX REIG y Coord. A. JAREÑO LEAL), Iustel, Madrid, 2010.

PRATS ALBENTOSA, L., “Principios de protección de datos: Calidad de los datos, consentimiento para el tratamiento de datos y deber de información” en *Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (aprobado por RD 1720/20079, de 21 de diciembre)*, (Dir. A. PALOMAR OLMEDA y P. GONZÁLEZ-ESPEJO), Thomson-Civitas, Cizur Menor, Navarra, 2008.

REBOLLO DELGADO, L., *La imagen como dato*. Anuario Facultad de Derecho.

TÉLLEZ AGUILERA, A., *Nuevas Tecnologías. Intimidad y Protección de Datos*, Edisofer SL, Madrid, 2001.

TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

- “Hacia un nuevo marco jurídico europeo de la protección de datos personales”, *Revista Española de Derecho Europeo*, nº 43, julio-septiembre 2012, pp. 25-184.

- “La protección de los datos sanitarios del menor”, en *Nuevos retos que plantean los menores en Derecho. III Jornadas sobre Derecho de los menores*, (Coords. I. E. LÁZARO GONZÁLEZ e I. V. MAYORAL NARROS), Publicaciones de la Universidad Pontificia de Comillas, Madrid, 2004.

VÁZQUEZ DE CASTRO, E., “Protección de datos personales, redes sociales y menores”, *Revista de Aranzadi de Derecho y Nuevas Tecnologías*, nº 29, 2012, pp. 54-58.

SEMPERE SAMANIEGO J., *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, libro publicado mediante Licencia Creative Commons Reconocimiento- No Comercial- Compartir igual CC BY-NC- SA, <http://es.linkedin.com/pub/fco-javier-sempere-samaniego/19/4bb/bba>.